

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем**

«На правах рукопису»
УДК 621.39

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«__» _____ 2020 р.

**Магістерська дисертація
на здобуття ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
на тему: «Дослідження впливу протоколів маршрутизації на надійність
телекомунікаційної мережі»**

Виконав (-ла):
студент (-ка) VI курсу, групи ТС-91мп
Вітковський Владислав Ігорович

Керівник:
доцент кафедри, кандидат технічних наук
Гаттуров Віктор Кавич

Рецензент:
доцент кафедри, кандидат технічних наук
Мазор Сергій Юрійович

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент (-ка) _____

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1
«Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___» _____ 20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Вітковському Владиславу Ігоровичу

1. Тема дисертації «Дослідження впливу протоколів маршрутизації на надійність телекомунікаційної мережі», науковий керівник дисертації Гаттуров Віктор Кавич, доцент, кандидат технічних наук, затверджені наказом по університету від «___» _____ 20__ р. № _____
2. Термін подання студентом дисертації 9 грудня 2019 року.
3. Об'єкт дослідження: телекомунікаційна мережа змодельована в програмному середовищі СРТ.
4. Предмет дослідження: комплекс питань, пов'язаних з впливом протоколів маршрутизації на надійність телекомунікаційної мережі та підвищенням відмовостійкості мережі, шляхом використання додаткового мережевого протоколу при спільній роботі з протоколом маршрутизації.
5. Перелік завдань, які потрібно розробити:
 1. Аналіз впливу топології на надійність мережі при побудові її архітектури;
 2. Аналіз впливу протоколів маршрутизації на надійність

телекомунікаційної мережі;

3. Дослідити функціональні властивості протоколів маршрутизації та їх вплив на надійність телекомунікаційної мережі;
4. Дослідити функціональні властивості додаткових мережевих технологій та їх вплив на надійність мережі при спільній роботі з протоколом маршрутизації;
6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Слайд 1 «Тема, мета, актуальність, об'єкт, предмет, проблематика, завдання дослідження»

Слайд 2 «Топологія і архітектура мережі»

Слайд 3 «Протоколи маршрутизації, що використовуються в мережі для забезпечення її надійності»

Слайд 4 «Мережеві технології, що використовуються в мережі для підвищення її надійності»

Слайд 5 «Порівняльний аналіз і підсумовування результатів дослідження»

Слайд 6 «Висновки»

7. Орієнтовний перелік публікацій

ВІТКОВСЬКИЙ В.І., КЕР. ГАТТУРОВ В. К. ДОСЛІДЖЕННЯ ВПЛИВУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ПРІТС 2020. - К.: КПІ ім. Ігоря Сікорського, 2020.

8. Дата видачі завдання 2 вересня 2019 року.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз літературних джерел по тематиці роботи	07.09.2019 - 06.10.2019	Виконано
2	Формулювання теми, мети, об'єкту та предмету дослідження у магістерській роботі	07.10.2019 - 18.11.2019	Виконано
3	Формулювання проблематики та визначення актуальності магістерської роботи. Зв'язок тематики магістерської роботи із сучасними інноваційними трендами в інформаційному середовищі	19.11.2019 - 02.01.2020	Виконано
4	Формування структури магістерської роботи	03.01.2020 - 05.03.2020	Виконано
5	Формування вступної частини та наповнення теоричної частини	06.03.2020 - 07.06.2020	Виконано
6	Проведення досліджень для вирішення наукових завдань	08.06.2020 - 22.09.2020	Виконано
7	Формування кінцевої структури магістерської роботи	23.09.2020 - 13.11.2020	Виконано
8	Формування кінцевих висновків та списку використаних літературних джерел	14.11.2020 - 28.11.2020	Виконано
9	Оформлення пояснювальної записки дипломної роботи	29.11.2020 - 04.12.2020	Виконано
10	Підготовка до захисту дипломної роботи	05.12.2020 - 10.12.20	Виконано

Студент

В.І. Вітковський

Науковий керівник дисертації

В.К. Гаттуров

РЕФЕРАТ

Темою магістерської дисертації є дослідження впливу протоколів маршрутизації на надійність телекомунікаційної мережі.

Робота містить 81 сторінку, зокрема 22 рисунків та 14 джерел інформації.

Актуальність теми обумовлена, розширенням цифрового середовища та існуючими відмовами в мережах, які порушують здійснення передачі мережевого трафіку до кінцевих користувачів.

Мета даної роботи полягає у забезпеченні надійності телекомунікаційної цифрової мережі та зменшення впливу аварійних ситуацій на надійність телекомунікаційної мережі за допомогою різних протоколів маршрутизації та додаткових мережевих протоколів.

Об'єкт дослідження: телекомунікаційна цифрова мережа змодельована у програмному середовищі Cisco Packet Tracer.

Предмет дослідження: функціональні можливості протоколів динамічної маршрутизації, їх вплив на надійність телекомунікаційної мережі та можливість підвищити надійність мережі за допомогою додаткового мережевого протоколу.

ABSTRACT

The relevance of the topic is due to the expansion of the digital environment and the existing failures in networks that disrupt the transmission of network traffic to end users.

The purpose of this work is to ensure the reliability of the telecommunications digital network and reduce the impact of emergencies on the reliability of the telecommunications network through various routing protocols and additional network protocols.

Object of research: digital telecommunication network is modeled in the Cisco Packet Tracer software environment.

Subject of research: functional capabilities of dynamic routing protocols, their impact on the reliability of the telecommunications network and the ability to increase network reliability with an additional network protocol.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	9
ВСТУП.....	11
1 НАДІЙНІСТЬ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ.....	13
1.1 Принципи побудови сучасних телекомунікаційних мереж.....	13
1.2 Телекомунікаційні мережі та їх класифікація.....	19
1.3 Параметри надійності в телекомунікаційній мережі.....	20
1.4 Методи для забезпечення та підвищення надійності телекомунікаційної мережі.....	22
1.5 Висновки до розділу 1	25
2 ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ	26
2.1 Основні принципи маршрутизації.....	27
2.2 Вимоги мережі до протоколу маршрутизації.....	33
2.3 Аналіз використання протоколів динамічної маршрутизації.....	34
2.4 Висновки до розділу 2	38
3 АНАЛІЗ ЗАСТОСУВАННЯ ДИНАМІЧНИХ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В СИСТЕМАХ ДЛЯ ПІДВИЩЕННЯ ТА ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ МЕРЕЖІ	41
3.1 Аналіз використання дистанційно-векторних протоколів маршрутизації	41
3.1.1 Протокол RIP	42
3.1.2 Протокол IGRP	43
3.1.3 Протокол EIGRP.....	44
3.1.4 Протокол BGP.....	45
3.2 Аналіз використання протоколів маршрутизації за станом каналів.....	46
3.2.1 Протокол OSPF.....	47
3.2.2 Протокол IS-IS	49
3.3 Аналіз застосування додаткових мережевих технологій для підвищення надійності мережі	49
3.3.1 Протокол HSRP	50

3.3.2 Протокол ESMTP	51
3.3.3 Протокол SNMP	52
3.3.4 Протокол VRRP	53
3.3.5 Протокол GLBP	55
3.4 Висновки до розділу 3	56
4 ДОСЛІДЖЕННЯ ВПЛИВУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	58
4.1 Дослідження впливу дистанційно-векторних протоколів маршрутизації	59
4.1.1 Модель з використанням протоколу RIP	59
4.1.2 Модель з використанням протоколу IGRP	61
4.2 Дослідження впливу протоколів маршрутизації за станом каналів	63
4.3 Порівняльний аналіз протоколів маршрутизації на основі досліджень з використанням ПС Cisco Packet Tracer	65
4.4 Дослідження впливу на надійність телекомунікаційної мережі та порівняльний аналіз додаткових мережевих технологій.....	66
4.5 Дослідження впливу протоколу маршрутизації OSPF з використанням додаткового мережевого протоколу	74
4.6 Висновки до розділу 4	75
ВИСНОВКИ.....	78
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	80

ПЕРЕЛІК СКОРОЧЕНЬ

- AS — Autonomous System — автономна система
- BGP — Border Gateway Protocol — Протокол граничного шлюзу
- CIDR — Classless Interdomain Routing — безкласова маршрутизація
- DV — Distance Vector — дистанційно-векторний (алгоритм маршрутизації)
- EIGRP — Enhanced Interior Gateway Routing Protocol — покращений протокол маршрутизації внутрішнього шлюза
- FIB — Forwarding Information Base — база даних комутації
- ICMP — Internet Control Message Protocol — протокол міжмережових керуючих повідомлень
- IP — Internet Protocol — міжмережовий протокол
- IS-IS — Intermediate System to Intermediate System — протокол “проміжна система — проміжна система”
- LAN — Local Area Network — локальна обчислювальна мережа
- LSA — Link State Advertisement — анонс стану каналу
- LSP — Label Switched Path — шлях комутований за мітками
- MAC — Media Access Control — каналний рівень моделі OSI
- OSPF — Open Shortest Path First — відкритий протокол “найкоротший шлях — перший”
- STP — Spanning Tree Protocol — протокол покриваючого дерева
- SVI — Switch Virtual Interface — віртуальний інтерфейс комутатора
- TCP — Transport Control Protocol — протокол управління передачею
- TLV — Type-Length-Value — поле пакету “тип-довжина-значення”
- WAN — Wide Area Network — глобальна обчислювальна мережа
- RIP — Routing Information Protocol — протокол маршрутної інформації
- IGRP — Interior Gateway Routing Protocol — протокол маршрутизації внутрішніх шлюзів
- GLBP — Gateway Load Balancing Protocol — протокол балансування навантаження шлюзу

SNMP — Simple Network Management Protocol — протокол управління мережевими пристроями

HSRP — Hot Standby Router Protocol — протокол маршрутизатора гарячого режиму очікування

VRRP — Virtual Router Redundancy Protocol — протокол резервування віртуального маршрутизатора

ECMP — Equal-Cost Multi-Path Routing — багатокільцева маршрутизація з рівною вартістю

AVF — Active Virtual Forwarder — активний віртуальний експедитор

AVG — Active Virtual Gateway — активний віртуальний шлюз

IS — Information Systems - інформаційні системи

VR — Virtual Router - віртуальний роутер

ВСТУП

Сьогодні ми спостерігаємо переломний момент у використанні технологій, які розширюють наші можливості спілкування. Швидкість глобалізації Інтернету перевершила всі очікування. Способи соціального, комерційного, політичного і особистого взаємодії дуже швидко змінюються, щоб не відставати від темпів еволюції глобальної мережі. На наступній стадії розробники будуть використовувати Інтернет в якості основи для створення нових продуктів і послуг, які використовують всі переваги мережі. У міру втілення в життя все нових і нових проектів, які здавалися раніше недосяжними, можливості об'єднаних мереж, що утворюють Інтернет, будуть грати все зростаючу роль в реалізації цих проектів.

Мережі дозволяють людям спілкуватися, співпрацювати і по-різному взаємодіяти. Мережі використовуються для відкриття веб-сторінок, спілкування через IP-телефони, участі у відеоконференціях, онлайн-ігор, здійснення покупок через Інтернет, дистанційного навчання та багато чого іншого.

Масштаб мереж даних, які ми використовуємо в повсякденному житті для навчання, роботи або в розважальних цілях, варіюється від невеликих локальних мереж до великих глобальних об'єднаних мереж. У домашніх умовах користувач може встановити маршрутизатор, а також два або більше комп'ютерів. В рамках організації мова може йти про використання декількох маршрутизаторів і комутаторів, що забезпечують обмін даними між сотнями або навіть тисячами комп'ютерів.

Маршрутизатор використовується для підключення однієї мережі до іншої. Маршрутизатор відповідає за доставку пакетів в різні мережі. Пунктом призначення для IP-пакета може бути веб-сервер, розташований в іншій країні, або сервер електронної пошти в локальній мережі.

Маршрутизатори виконують пересилання пакетів, використовуючи дані таблиці маршрутизації. Інформацію про маршрути до віддалених мереж маршрутизатор отримує за допомогою статичних і динамічних маршрутів.

У великій мережі, що складається з декількох мереж і підмереж, налагодження та обслуговування статичних маршрутів між цими мережами вимагає частого адміністративного втручання і значних непродуктивних витрат. Непродуктивні витрати особливо зростають при необхідності внесення змін до мережі, наприклад, при збої в роботі каналу або реалізації нової підмережі. Використання протоколів динамічної маршрутизації може зменшити обсяг завдань по налаштуванню і обслуговуванню і забезпечити більшу масштабованість мережі.

1 НАДІЙНІСТЬ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Принципи побудови сучасних телекомунікаційних мереж

У наш час основною тенденцією проектування та побудови телекомунікаційних мереж стала так звана «Трирівнева модель організації мережі».

Інженери розробили трирівневу систему ієрархічну модель мережі(рис.1.1). Вона логічна і за рахунок апаратної надмірності дає високу ступінь надійності.

Мережа була розділена на три рівні:

1. Ядро мережі (Core layer)
2. Рівень розподілу (Distribution layer)
3. Рівень доступу (Access layer)

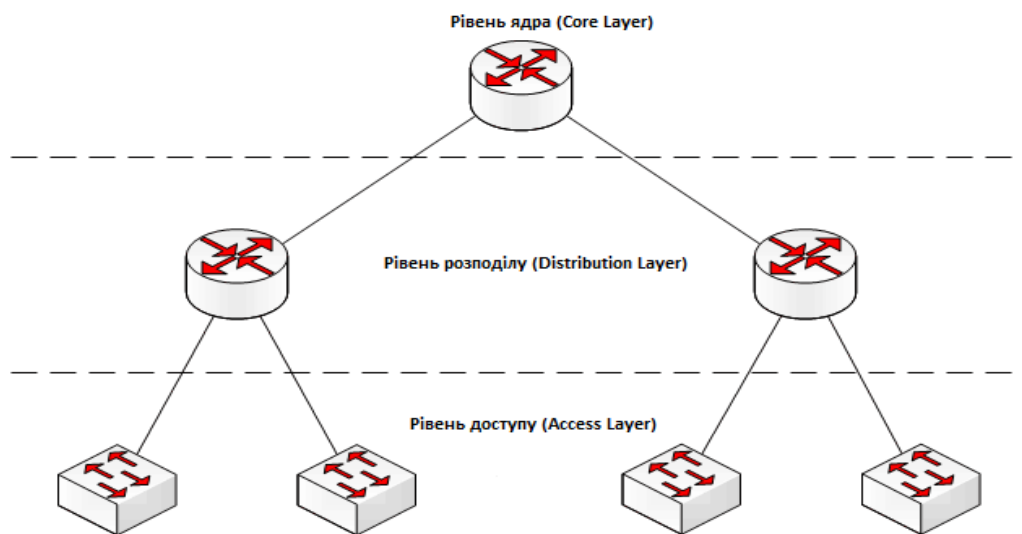


Рисунок 1.1 Трирівнева ієрархічна модель організації мережі

1. Рівень ядра, базовий рівень - формує ядро мережі. На самому верху ієрархії цей рівень відповідає за швидку і надійну пересилку великих об'ємів трафіку та з'єднання мережі з мережами інших провайдерів.

Якщо відбувається помилка на базовому рівні, то вона впливає на всіх користувачів. Отже, важливо забезпечити високу надійність на базовому рівні. На цьому рівні обробляються великі обсяги трафіку, тому не менш важливо

враховувати швидкість і затримки. На цьому рівні доречно буде використовувати повнозв'язну топологію.

2. Рівень розподілу, рівень робочих груп - розташований між базовим рівнем(рівень ядра) та рівнем доступу.

Рівень розподілу зобов'язаний встановлювати найбільш швидкий спосіб обробки запитів до служб. Після визначення на рівні розподілу найкращого шляху доступу, запит може бути переданий на базовий рівень, де реалізований швидкісний транспорт запиту до потрібної служби.

Основні функції рівня розподілу складаються в маршрутизації, фільтрації і доступі до регіональних мереж, а також (якщо необхідно) у визначенні правил доступу пакетів до базового рівня. Топологія цього рівня – кільце або подвійне кільце.

3. Рівень доступу - на рівні доступу реалізовано управління користувачами і робочими групами при зверненні до ресурсів об'єднаної мережі. До рівня доступу безпосередньо фізично приєднуються самі користувачі.

Топологія цього рівня – деревовидна.

Під топологією мережі розуміється опис її фізичного розташування, а саме, як комп'ютери з'єднані один з одним в мережі, і за допомогою яких пристроїв входять в фізичну топологію. Існують чотири основних топології: шина (Bus), кільце (Ring), зірка (Star) і Mesh-мережі (Mesh). Інші топології зазвичай є комбінацією двох і більше головних типів.

Вибір типу фізичної топології для мережі є одним з перших кроків планування мережі. Вибір топології ґрунтується на безлічі факторів, у число яких входять ціна, відстані, питання безпеки, передбачувана мережева операційна система, а також чи буде нова мережа використовувати існуюче обладнання, проводку і т.п.

Фізична топологія "шина" (Bus), що іменується також лінійною шиною (Linear Bus), складається з єдиного кабелю, до якого приєднані всі комп'ютери сегмента (рис.1.2). Повідомлення надсилаються на лінії всім підключеним станціям незалежно від того, хто є одержувачем. Кожен комп'ютер перевіряє

кожен пакет в дроті, щоб визначити одержувача пакета. Якщо пакет призначений для іншої станції, комп'ютер відкине його. Відповідно, комп'ютер отримає і обробить будь-який пакет на шині, адресований йому.

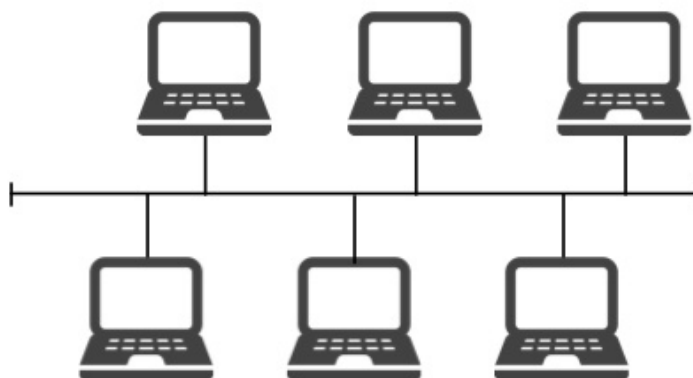


Рисунок 1.2 Топологія «Шина»

Головний кабель шини, відомий як магістраль (backbone), має на обох кінцях заглушки (terminator) для запобігання відображення сигналу. Без правильно встановлених заглушок робота шини буде ненадійною або взагалі неможливою.

Шинна топологія представляє собою найшвидший і найпростіший спосіб установки мережі. Вона вимагає менше обладнання та кабелів, ніж інші топології, і її легше налаштовувати. Це хороший спосіб швидкого побудови тимчасової мережі. Це зазвичай кращий вибір для малих мереж (не більше 10 комп'ютерів).

Є кілька недоліків, про які треба знати при вирішенні питання про використання шинної топології для мережі. Неполадки станції або іншого компонента мережі важко ізолювати. Крім того, неполадки в магістральному кабелі можуть привести до виходу з ладу всієї мережі.

Топологія "кільце" (Ring) зазвичай використовується в мережах Token Ring і FDDI (волоконно-оптичних). У фізичній топології Ring лінія передачі даних фактично утворює логічне кільце, до якого підключені всі комп'ютери мережі (рис.1.3). На відміну від шинної топології, яка використовує конкурентну схему,

щоб дозволити станціям отримувати доступ до мережевого носія, доступ до носія в кільці здійснюється за допомогою логічних знаків - "маркерів" (token), які пускаються по колу від станції, до станції, даючи їм можливість переслати пакет, якщо це потрібно. Це дає кожному комп'ютеру в мережі рівну можливість отримати доступ до носія і, отже, переслати по ньому дані. Комп'ютер може посилати дані тільки тоді, коли володіє маркером.

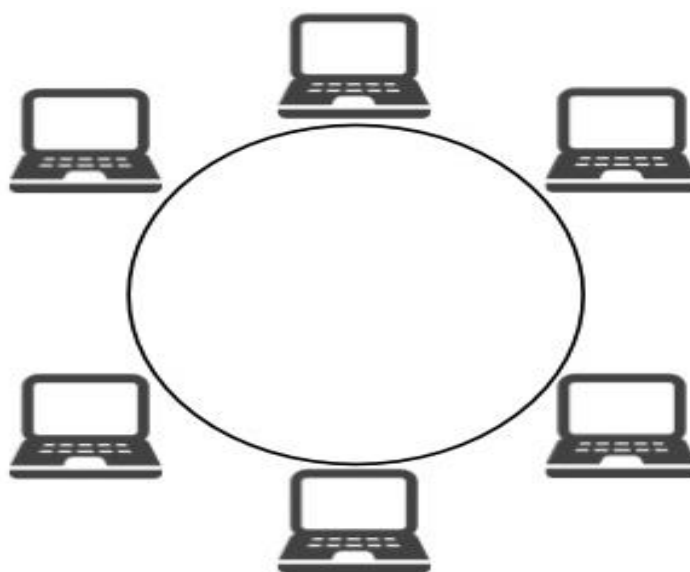


Рисунок 1.3 Топологія «Кільце»

Так як кожен комп'ютер при цій топології є частиною кільця, він має можливість пересилати будь-які отримані ним пакети даних, адресовані іншій станції. Що виходить регенерація робить сигнал сильним і дозволяє уникнути необхідності в застосуванні повторителів. Так як кільце формує нескінченний цикл, заглушки не потрібні. Кільцева топологія щодо легка для установки і настройки, вимагаючи мінімального апаратного забезпечення.

Топологія фізичного кільця має кілька недоліків. Як і в разі лінійної шини, неполадки на одній станції можуть привести до відмови всієї мережі. Підтримувати логічне кільце важко, особливо в великих мережах. Крім того, в разі необхідності настройки і переконфігурації будь-якій частині мережі доведеться тимчасово відключити всю мережу.

Кільцева топологія дасть всім комп'ютерам рівні можливості доступу до мережевого носія.

У топології "зірка" (Star) всі комп'ютери в мережі з'єднані один з одним за допомогою центрального концентратора (рис.1.4). Всі дані, які посилає станція, прямують прямо на концентратор, який потім пересилає пакет в напрямку одержувача. Як і при шинної топології, комп'ютер в мережі типу "зірка" може намагатися надіслати дані в будь-який момент. Однак на ділі тільки один комп'ютер може в конкретний момент часу проводити посилку. Якщо дві станції посилають сигнали на концентратор точно в один час, обидві посилки виявляться невдалими і кожному комп'ютеру доведеться почекати випадковий період часу, перш ніж знову намагатися отримати доступ до носія. Мережі з топологією Star зазвичай краще масштабуються, ніж інші типи.

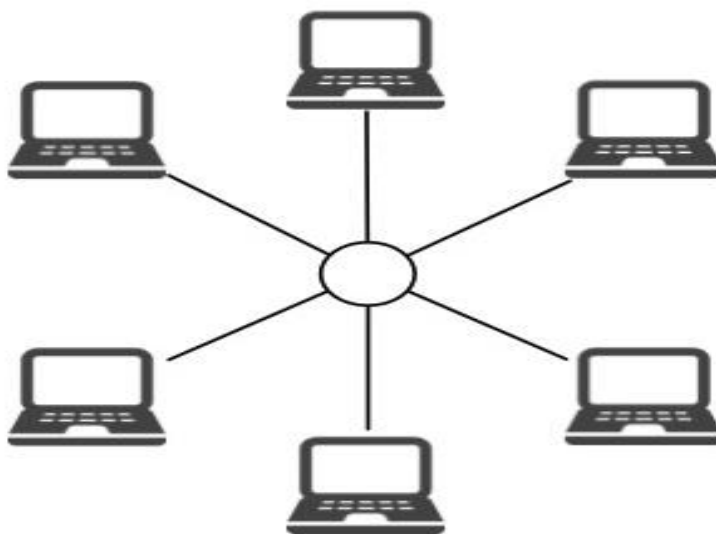


Рисунок 1.4 Топологія «Зірка»

Головна перевага впровадження топології "зірка" полягає в тому, що на відміну від лінійної шини неполадки на одній станції не виведуть з ладу всю мережу. У мережах з цієї топологією простіше знаходити обриви кабелю та інші несправності. Це полегшує виявлення обриву кабелю з іншими проблемами. Крім того, наявність центрального концентратора в топології "зірка" полегшує додавання нового комп'ютера і реконфігурацію мережі.

Топології "зірка" притаманне кілька недоліків. По-перше, цей тип конфігурації вимагає більше кабелю, чим більшість інших мереж, внаслідок наявності окремих ліній, що з'єднують кожен комп'ютер з концентратором. Крім того, центральний концентратор виконує більшість функцій мережі, так що вихід з ладу одного цього пристрою відключить всю мережу.

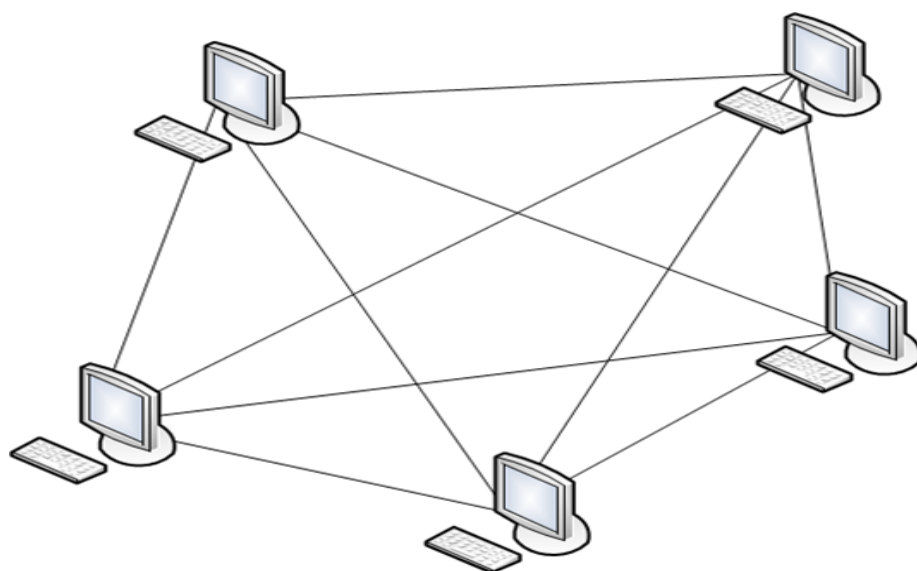


Рисунок 1.5 Топологія «Комірчаста»

Mesh-мережі (Mesh) з'єднує всі комп'ютери попарно (рис. 1.5). Мережі повнозв'язної топології використовують значно більше кабелю, чим будь-яка інша топологія, що робить їх дорожче. Крім того, такі мережі значно складніше встановлювати, ніж інші топології. Однак Mesh-мережі стійка до збоїв (fault tolerance). Стійкість до збоїв полягає в здатності працювати при наявності пошкоджень. У мережі з пошкодженим сегментом це означає обхід сегмента. Кожен комп'ютер має безліч можливих шляхів сполучення з іншим комп'ютером по мережі, так що окремий обрив кабелю не призведе до втрати з'єднання між будь-якими двома комп'ютерами.

1.2 Телекомунікаційні мережі та їх класифікація

Телекомунікації - це будь-які форми зв'язку, способи передачі інформації на великі відстані. Телекомунікації - це також процеси передачі, отримання та обробки інформації на відстані із застосуванням електронних, електромагнітних, мережевих, комп'ютерних та інформаційних технологій.

Однією з основних характеристик телекомунікаційної мережі є надання можливості отримання необхідної інформації для забезпечення діяльності фірми чи задоволення особистих потреб користувачів.

Проблема інформаційного наповнення телекомунікаційних мереж стає все більш важливою в зв'язку тенденціями розвитку світової інформаційної інфраструктури. Існуючі на сьогоднішній день кілька десятків мереж не можуть набрати необхідну кількість абонентів для самоокупності та стабільної діяльності. Тому гостро постає питання про комплексне обслуговування користувача. Необхідно відзначити також проблему якості баз даних та інформаційно-пошукових систем.

Типи телекомунікаційних систем.

За призначенням телекомунікаційні системи групуються наступним чином:

- системи телемовлення;
- системи зв'язку (в т.ч. персонального виклику);
- комп'ютерні мережі.
- За типом використовуваного середовища передачі інформації:
 - кабельні (традиційні мідні);
 - оптоволоконні;
 - ефірні;
 - супутникові.

За способом передачі інформації:

- аналогові;
- цифрові.

Системи зв'язку поділяються за мобільністю на:

- стаціонарні (традиційні абонентські лінії);
- рухливі.

Рухливі системи зв'язку поділяються за принципом охоплення зони обслуговування:

- на мікростільникові - GSM;
- стільникові - GSM, CDMA, GPRS, WCDMA, LTE;
- транкінгові - TETRA, SmarTrunk;
- супутникові.

Як показує практика, навіть підготовленому користувачеві дуже важко оцінити параметри представлених систем. Доводиться з жалем констатувати, що нерідко найвідоміші з реклами системи не є дійсно найкращими, так як іноді велика частина зусиль виробника інформаційної продукції зосереджена на організації рекламної діяльності, а проблеми якості товарів, що поставляються залишаються на другому плані. Тому безсумнівний інтерес для під час виборів інформаційних систем представляють дані, отримані досвідченими експертами на конкурсах інформаційних систем.

Для досліджень, буде використана модель цифрової комп'ютерної мережі.

1.3 Параметри надійності в телекомунікаційній мережі

Телекомунікаційні мережі характеризують за показниками, які відображають у цілому можливість і ефективність транспортування інформації. Можливість транспортування інформації в телекомунікаційній мережі пов'язана зі ступенем її функціональності в часі, тобто виконанням заданих функцій в повному обсязі з необхідним рівнем якості протягом певного періоду експлуатації мережі або в конкретний момент часу.

Працездатність мережі пов'язана з поняттями надійності та живучості. Різниця між цими поняттями зумовлена, насамперед, відмінностями причин та факторів, які порушують нормальну роботу мережі, та специфікою порушень.

Надійність мережі зв'язку характеризується здатністю забезпечувати зв'язок, зберігаючи в часі значення встановлених показників якості в заданих умовах експлуатації.

Вона відображає вплив на працездатність мережі передусім внутрішніх чинників: випадкових відмов технічних засобів, спричинених процесами старіння, дефектами технології виготовлення або помилками обслуговуючого персоналу. Показниками надійності є, наприклад, відношення часу працездатності мережі до загального часу її експлуатації, ймовірність безвідмовного зв'язку та ін.

Важливим показником є також кількість незалежних шляхів передавання інформаційного повідомлення, які можуть бути визначені між парою пунктів мережі.

Живучість мережі зв'язку характеризується здатністю зберігати повну або часткову функціональність під впливом руйнуючих причин, які виникають поза межами мережі й призводять до виходу з ладу чи значних пошкоджень деякої частини її елементів (пунктів і ліній зв'язку). Виокремлюють два типи таких причин: стихійні й навмисні. До стихійних чинників відносяться: землетрус, повіні та інші форсмажорні обставини, до навмисних – пошкодження мережі в наслідок злочинних дій.

Живучість мережі можуть характеризувати такі показники, які визначають: вірогідність того, що між будь якою заданою парою пунктів мережі можна передати обмежений обсяг інформації після впливу руйнівних факторів; мінімальну кількість пунктів, ліній мережі (або тих та інших), вихід з ладу яких призводить до порушення зв'язності мережі відносно довільної пари пунктів; середню кількість пунктів, які залишаються зв'язними при одночасному пошкодженні декількох ліній зв'язку та ін.

Пропускна здатність мережі. У тих випадках, коли мережа не може обслуговувати (реалізувати) необхідне навантаження, говорять про обсяг реалізованого навантаження в мережі. Величина реалізованого мережею навантаження визначає її пропускну здатність і в ряді випадків може бути оцінена кількісно апіорі. Наприклад, можна визначити величину максимального потоку

інформації між двома пунктами (джерело-стік), або пропускну спроможність перетину мережі, що є найвужчим місцем при поділі мережі між джерелом і стоком на дві частини. Оцінка пропускну здатності мережі значною мірою пов'язана з параметрами якості обслуговування, тому що реалізація конкретного навантаження має здійснюватися відповідно до заданих параметрів якості.

Якість обслуговування визначається сукупністю показників, які вказують на рівень відповідності телекомунікаційної мережі нормам експлуатації та вимогам користувачів.

Рентабельність і вартість. Телекомунікаційна мережа є рентабельною, як що витрати на її організацію і забезпечення працездатності окупаються доходом від наданих користувачам послуг. Основна економічна характеристика мережі - це зведені (загальномережеві) витрати, які визначають її вартість з урахуванням експлуатації й керування.

1.4 Методи для забезпечення та підвищення надійності телекомунікаційної мережі

Отже, під надійністю прийнято розуміти комплекс властивостей інформаційних систем(ІС), які забезпечують виконання заданих функцій зі збереженням у часі і в заданих обмеженнях експлуатаційних характеристик. Характеристики визначаються показниками, які піддаються контролю і обліку.

В основному в комплекс властивостей надійності інформаційних систем, входять наступні властивості:

- безвідмовність - властивість зберігати працездатність протягом деякого часу;
- стійкість - властивість зберігати працездатність в умовах дії перешкод;
- коректність - властивість, що полягає в пристосованості до попередження і виявлення причин виникнення відмов, пошкоджень та

підтримці і відновленню працездатного стану шляхом доопрацювання і модернізації;

– захищеність - властивість про неможливість реалізації сторонніх втручань.

Наведені вище властивості надійності чисельно виражаються через показники надійності - кількісні характеристики одного або декількох властивостей, що визначають надійність ІС.

Сучасний етап розвитку територіально розподілених мереж передачі даних характеризується зростанням складності і масштабів інфраструктур, безперервним підвищенням вимог до якості послуг, що надаються зв'язку, доступу до сервісів. Мережа передачі даних повинна бути економічно ефективною, і при її проектуванні або модернізації має бути виконано відповідне обґрунтування та надані розрахунки щодо забезпечення надійності. До надійності мереж пред'являються все більш високі вимоги. Низька надійність призводить до втрати клієнтів, збитків і штрафних санкцій.

Підвищення надійності мережі пов'язано з додатковими витратами, які можуть перевищити прибуток, одержуваний від надання інфокомунікаційних послуг. У зв'язку з цим актуальною є задача досягнення необхідних характеристик надійності при проектуванні або модернізації мережі при мінімально можливих витратах на її забезпечення. Під терміном «надійність» розуміється властивість мережі зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах використання.

Надійність мережі забезпечується застосуванням надійного обладнання і внесенням надмірності в структуру мережі для підвищення готовності мережі, тобто, забезпечення її відмовостійкості.

Комплексне вирішення завдань забезпечення надійності включає обидва напрямки - забезпечення апаратної та структурної надійності. У першому випадку вирішується проблема забезпечення надійності елементів мережі - мережевого обладнання, каналів передачі даних, програмного забезпечення. Структурна

надійність забезпечує функції мережі, пов'язані з передачею даних. Для аналізу структурної надійності використовуються показники зв'язності граф-моделей мережі.

Порушити зв'язність може як відмова апаратури в вузлах мережі, так і відмова каналів передачі даних. При цьому відмова каналу може бути пов'язаний як з його механічним пошкодженням (обривом), так і з погіршенням його характеристик, в тому числі перевищенням його пропускну здатності. Для забезпечення зв'язності мережі застосовуються відмовостійкі мережеві технології, пов'язані з введенням надмірності реалізацією обхідних шляхів передачі інформації, і застосуванням протоколів, наприклад STP, автоматично забезпечують обхід відмовив ділянки.

Внесення надмірності в топологію корпоративних мереж дозволяє підвищити надійність маршрутизації великих обсягів трафіку, забезпечивши зв'язність з максимальним числом зовнішніх мереж.

Для реалізації підвищення надійності необхідно розвивати складні комп'ютерні мережі (КМ) як державного рівня, так і рівня підприємств. При цьому сегменти КМ можуть перебувати в різних регіонах країни на значній відстані один від одного. Створення окремої телекомунікаційної мережі для кожної КМ не представляється можливим як з економічних, так і з технічних причин. Таким чином, необхідна інтеграція з мережею зв'язку загального користування і можна говорити про те, що переважна більшість сучасних комп'ютерних мереж інтегровані з мережею Інтернет.

Це призводить до серйозного підвищення ризику виходу елементів мережі з ладу в результаті впливу навмисних і ненавмисних перешкод. Наслідком відмови безлічі елементів мережі може стати руйнування комп'ютерної мережі та неможливість здійснювати інформаційний обмін.

Основними напрямками забезпечення надійності передачі інформації є: нарощування додаткових ресурсів в мережі передачі даних, різні способи маршрутизації, порівняльний аналіз оцінки надійності структур на етапі проектування. Нарощування додаткових ресурсів з метою резервування каналу на

випадок підвищення кількості переданих повідомлень є дорогим рішенням. Маршрутизація дозволяє розподіляти трафік по різних каналах і вузлів, компенсуючи його зростання.

1.5 Висновки до розділу 1

В першому розділі, було розглянуто принципи побудови сучасних телекомунікаційних мереж та типи фізичних топологій, які використовуються у наш час в цифровому просторі. Також, було розглянуто типи телекомунікаційних мереж та їх класифікація.

Виходячи з вищесказаного, можливо зробити висновок, що для підвищення надійності мережі варто використовувати надійне обладнання одного вендора, яке буде повністю сумісним з мережевими технологіями, що використовуються для маршрутизації трафіку та забезпечують виконання заданих функцій мережі.

Було обґрунтовано, що надійність телекомунікаційної мережі повинна забезпечувати клієнтам можливість обмінюватися інформацією і отримувати сервіси в умовах технічних відмов, експлуатаційних помилок, а також з урахуванням можливих загроз і ризиків, пов'язаних з атаками типу відмова в обслуговуванні. Для підвищення надійності мережі, пропонується метод внесення надмірності в структуру мережі, яка допоможе справлятися з раптовими аваріями в мережі, тобто, таким чином можна підвищити відмовостійкість мережі.

Для оцінки надійності мережі, буде використовуватися час відновлення вузла, шляхом використання ICMP запитів та фіксацією часу їх проходження по мережі, відправлених з одного вузла на інший при використанні різних протоколів маршрутизації та мережових технологій.

2 ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

Маршрутизація є функцією третього рівня моделі OSI. Вона заснована на ієрархічній схемі, яка дозволяє групувати окремі адреси і працювати з групами як з єдиним цілим до тих пір, поки не буде потрібно встановити індивідуальну адресу для остаточної доставки даних.

Під терміном "маршрутизація" мають на увазі процес визначення найефективнішого шляху від одного пристрою до іншого. Основним пристроєм, що відповідає за здійснення процесу маршрутизації, є маршрутизатор.

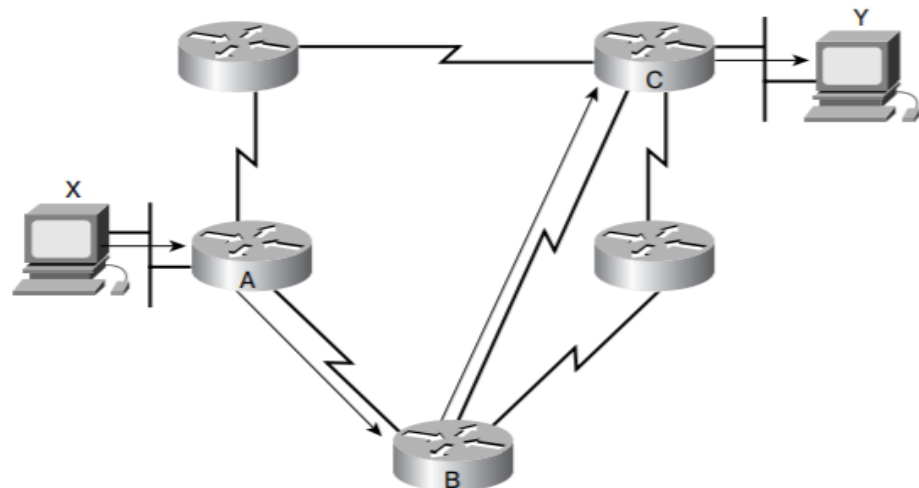


Рисунок 2.1 Принцип дії протоколу мережевого рівня

Маршрутизатор виконує дві ключові функції:

- підтримує таблиці маршрутизації і обмінюється інформацією про зміни в топології мережі з іншими маршрутизаторами. Ця функція реалізується за допомогою одного або декількох протоколів маршрутизації для передачі мережевої інформації іншим маршрутизаторів;
- коли пакети приходять на один з інтерфейсів, маршрутизатор, керуючись таблицею маршрутизації, повинен визначити, куди саме слід відправити пакет. Він перенаправляє пакети на обраний інтерфейс, створює фрейми і потім пересилає їх.

2.1 Основні принципи маршрутизації

Для передачі даних між різними мережами використовується маршрутизатор. Даний мережевий пристрій працює на мережевому рівні моделі OSI. Основними завданнями маршрутизатора є вибір найкращого маршруту до мережі призначення і комутація пакетів для передачі.

Використання маршрутизаторів передбачає, що мережа матиме складну структуру з різними технологіями передачі даних на канальному і фізичному рівнях і безліччю маршрутів, в тому числі з надлишковими зв'язками.

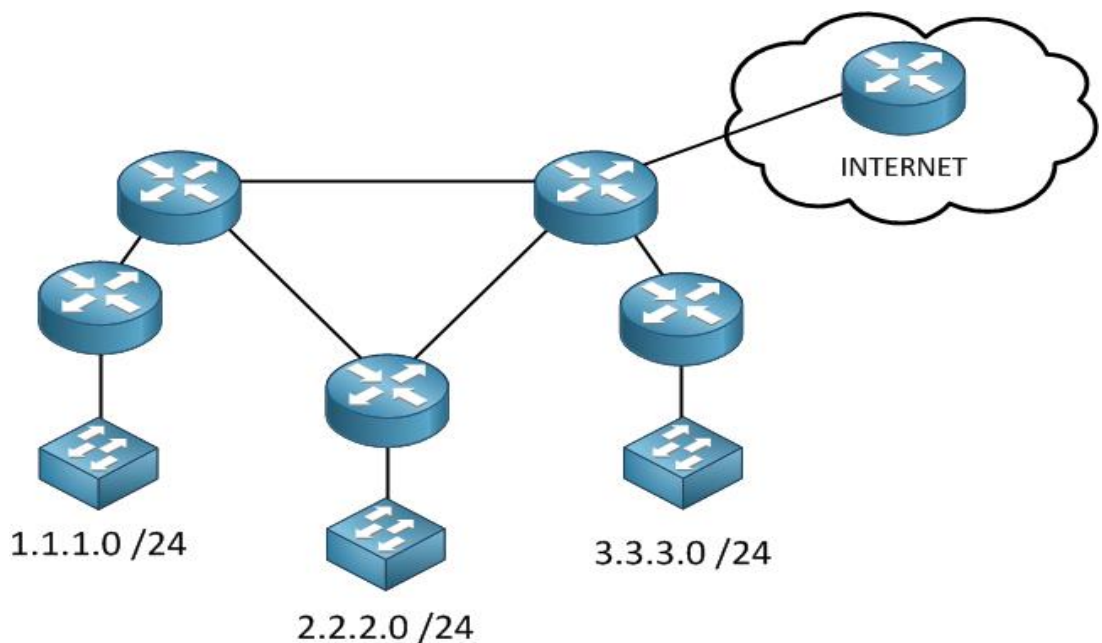


Рисунок 2.2 Принцип дії маршрутизаторів

Виходячи з цього, можна сказати наступне:

1. Маршрутизатор будує таблицю маршрутизації на підставі інформації, отриманої через свої інтерфейси, від сусідніх маршрутизаторів.
2. Маршрутизатор приймає рішення про передачу пакета, ґрунтуючись лише на інформації, яка міститься в його таблиці маршрутизації.

3. У мережі, побудованій на маршрутизаторах, інформація, яка передається до місця призначення по одному маршруту, назад може передаватися по іншому маршруту.

Коли пристрій має кілька шляхів для досягнення пункту призначення, воно завжди вибирає один шлях, вважаючи за краще його іншим. Цей процес вибору називається Routing. Маршрутизація виконується за допомогою спеціальних мережевих пристроїв, званих маршрутизаторами, або їх можна виконувати за допомогою програмних процесів. Маршрутизатор на основі програмного забезпечення мають обмежену функціональність і обмежену область дії.

Маршрутизатор завжди налаштований з певним маршрутом за замовчуванням. Маршрут за замовчуванням повідомляє маршрутизатора, куди пересилати пакет, якщо маршрут не знайдено для конкретного адресата. Якщо існує кілька шляхів для досягнення одного і того ж адресата, маршрутизатор може прийняти рішення на основі такої інформації:

- Кількість стрибків
- Пропускна здатність
- Метрика
- Довжина префікса
- Затримка

Мета маршрутизації - це вибір оптимального маршруту доставки даних з однієї мережі в іншу. Для забезпечення маршрутизації будуються спеціальні таблиці, які називаються таблицями маршрутизації.

Визначення маршруту може базуватися на різних показниках (величинах, результуючих з алгоритмічних обчислень по окремій змінній - наприклад, довжина маршруту) або комбінаціях показників. Програмні реалізації алгоритмів маршрутизації вираховують показники маршруту для визначення оптимальних маршрутів до пункту призначення.

Для полегшення процесу визначення маршруту, алгоритми маршрутизації ініціалізують і підтримують таблиці маршрутизації, в яких міститься маршрутна

інформація. Маршрутна інформація змінюється в залежності від використовуваного алгоритму маршрутизації.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

R 10.0.0.0/8 [120/1] via 192.168.1.2, 00:00:12, Serial0/0/0
R 11.0.0.0/8 [120/1] via 192.168.2.2, 00:00:02, Serial0/0/1
172.1.0.0/24 is subnetted, 2 subnets
C 172.1.1.0 is directly connected, FastEthernet0/0
C 172.1.2.0 is directly connected, FastEthernet0/1
C 192.168.1.0/24 is directly connected, Serial0/0/0
C 192.168.2.0/24 is directly connected, Serial0/0/1
R 192.168.3.0/24 [120/1] via 192.168.1.2, 00:00:12, Serial0/0/0
[120/1] via 192.168.2.2, 00:00:02, Serial0/0/1

R1#
```

Рисунок 2.3 Приклад таблиці маршрутизації

На рисунку (2.3) представлений приклад таблиці маршрутизації маршрутизатора фірми "Cisco".

У верхній частині, знаходиться довідкова інформація про джерела маршрутної інформації (як запис про маршрут потрапила в таблицю).

Рядок «Gateway of last resort is not set» вказує на наявність маршруту за замовчуванням. Решта рядків вказують номери «відомих» маршрутизатора мереж з визначенням способу отримання маршрутної інформації та уподобань маршруту.

Розглянемо докладніше рядок з таблиці маршрутизації R 10.0.0.0/8 [120/1] via 192.168.1.2, 00:00:12, Serial0 / 0/0

Інформація про маршрут, яка знаходиться в таблиці маршрутизації, містить наступні дані:

R - джерело отримання маршрутної інформації.

10.0.0.0/8 - номер (IP-адреса) мережі призначення і префікс (Mask).

[120/1] - параметри маршруту (адміністративна дистанція «120» і метрика - «1»).

Адміністративна дистанція визначає ступінь довіри до джерела маршрутної інформації. Метрика визначає вартість маршруту до мережі призначення і формується джерелом маршрутної інформації.

Якщо одне джерело маршрутної інформації отримає кілька маршрутів до мережі призначення, то в таблицю маршрутизації буде занесений маршрут з найменшою метрикою. Якщо до мережі призначення буде отримано кілька маршрутів від різних джерел, то в таблицю маршрутизації буде занесений маршрут з найменшим значенням даного параметра.

192.168.1.24 - IP-адреса інтерфейсу сусіднього маршрутизатора по шляху до мережі призначення (next hop).

00:00:12 - Час, що минув з моменту поновлення інформації по даному маршруту.

Serial0 / 0/0 - Ім'я вихідного інтерфейсу даного маршрутизатора для передачі пакета до мережі призначення.

Можна виділити три шляхи, по яких маршрутна інформація потрапляє в таблицю:

В першу чергу, в таблицю маршрутизації заносяться записи про мережах, які безпосередньо підключені до інтерфейсів маршрутизатора. Вони визначаються як «C» - connected (виділено зеленим). Вказується, що дана мережа є безпосередньо підключеною (is directly connected).

Зверніть увагу на те, що в цих маршрутах не вказані значення метрики і адміністративної дистанції. Для маршрутів даного типу значення цих параметрів дорівнюють нулю.

Другий шлях - за допомогою статичної маршрутизації. Маршрутизатор дізнається про маршрут, коли адміністратор налаштовує маршрут вручну (статично). В цьому випадку при зміні топології мережі записи про маршрутах повинні оновлюватися вручну. Тут так само не вказані значення метрики і адміністративної дистанції. Для маршрутів даного типу значення метрики - «0», а адміністративної дистанції (за замовчуванням) - «1».

Третій шлях - за допомогою динамічної маршрутизації.

Маршрутизатор динамічно вивчає маршрути, після того як на ньому налаштований протокол маршрутизації. Протокол маршрутизації автоматично оновлює маршрути при отриманні інформації про зміну мережевої топології.

Маршрутизатор вивчає і підтримує маршрути до віддалених мереж, обмінюючись оновленнями маршрутної інформації з іншими маршрутизаторами в мережі.

Тепер розглянемо, в якому порядку встановлюються записи про маршрутах в таблиці маршрутизації. Всі записи встановлюються в порядку зростання номера мережі призначення.

При цьому, якщо префікс (маска) номера мережі відповідає класу мережі, то такий маршрут записується в таблицю без доповнень.

В даному прикладі це маршрути в мережі 10.0.0.0, 11.0.0.0 і 192.168.3.0.

Якщо префікс більше класової маски мережі, то в таблиці створюється додаткова запис з класової маскою і зазначенням кількості підмереж, які «відомі маршрутизатора» і належать даному класу. Такий запис можна назвати батьківський маршрут.

В даному прикладі це 150.160.0.0/24 і 172.1.0.0/16.

Ті маршрути, номери мереж яких є підмережами для батьківських, називаються - спадкоємці.

У префікс батьківського маршруту вказується значення префікса спадкоємців (підмереж), якщо у всіх спадкоємців префікси рівні. Якщо у спадкоємців префікси різні, то батькові записується класовий префікс. Якщо до

мережі призначення відомо кілька маршрутів з однаковою метрикою, то вони записуються один за одним.

Існує багато способів вирішення задач пошуку оптимальних шляхів в мережі, що реалізовані в протоколах, за якими відбувається маршрутизація. Ці протоколи поділяються на дві категорії: протоколи внутрішньої маршрутизації (IGP, Interior Gateway Protocols): OSPF (Open Shortest Path First), Dual IS-IS (Intermediate System to Intermediate System), RIP (Routing Information Protocol), GGP (Gateway to Gateway Protocol); та протоколи зовнішньої маршрутизації (Exterior Gateway Protocols): BGP (Border Gateway Protocol), EGP (Exterior Gateway Protocol), InterAS Routing without Exterior Gateway; та статична маршрутизація (Static Routing).

З математичної точки зору протоколи маршрутизації виконують пошук найменшого зв'язного дерева по графу, ребер якого відповідають наявним лініям зв'язку, а ваги ребер обчислюються відповідно до адміністративно заданих критеріїв.

У маршрутних таблицях може міститися також і інша інформація. "Показники" забезпечують інформацію про бажаність якого-небудь каналу або тракту. Роутери порівнюють показники, щоб визначити оптимальні маршрути. Показники відрізняються один від одного в залежності від використаної схеми алгоритму маршрутизації. Далі в цій главі буде представлений і описаний ряд загальних показників.

Роутери повідомляються один з одним (і підтримують свої маршрутні таблиці) шляхом передачі різних повідомлень. Одним з видів таких повідомлень є повідомлення про "відновлення маршрутизації". Оновлення маршрутизації зазвичай включають всю маршрутну таблицю або її частину. Аналізуючи інформацію про відновлення маршрутизації, що надходить від усіх роутерів, будь-який з них може побудувати детальну картину топології мережі. Іншим прикладом повідомлень, якими обмінюються роутери, є "об'явлення про стан каналу". Об'явлення про стан каналу інформує інші роутери про стан каналів відправника. Канальна інформація також може бути використана для побудови

повної картини топології мережі. Після того, як топологія мережі стає зрозумілою, роутери можуть визначити оптимальні маршрути до пунктів призначення.

2.2 Вимоги мережі до протоколу маршрутизації

Як відомо, протоколи динамічної маршрутизації дозволяють маршрутизаторам IP-мереж автоматично створювати таблиці оптимальних (за обраним критерієм) маршрутів і динамічно модифікувати їх відповідно до змін, що відбуваються в топології мережі.

Визначення протоколу для впровадження його в мережу, залежить від наступних факторів:

1. Фізична топологія мережі і її складність.

При побудові мережі, дуже важливо передбачити наявність резервних ліній зв'язку, які будуть забезпечувати надійне функціонування в разі відмов мережевого обладнання та основних ліній зв'язку.

2. Кількість мережевих вузлів в мережі і можливість її в масштабуванні в разі потреби.

Функціональні можливості деяких протоколів маршрутизації, можуть бути обмежені через розміри мережі.

3. Потенційна завантаженість мережі.

Велике значення має можливість протоколу маршрутизації до розподілу потоку трафіку по каналах зв'язку, в разі їх перевантаженості.

4. Певні вимоги до надійності функціонування мережі.

Час простоїв через відмови мережевих вузлів в мережі, залежить від роду діяльності організації, визначається можливими фінансовими збитками або порушенням виробничого циклу в компанії.

5. Вимоги до захисту інформації в мережі.

Ці вимоги визначаються ступенем ризику, пов'язаного з потраплянням конфіденційної інформації про логічних маршрутах мережі і її мережевих вузлів

в руки зловмисників, що особливо важливо для мереж, що мають зовнішні канали зв'язку.

6. Необхідність підключення маршрутизації сегмента до вже існуючої мережі.

В цьому випадку слід звернути увагу на сумісність протоколів маршрутизації і засобів їх реалізації.

7. Можливість організації програмних маршрутизаторів.

При невеликому трафіку в мережі або на окремих її ділянках від маршрутизаторів не потрібна висока продуктивність. У таких випадках з економічної точки зору буває вигідніше використовувати замість апаратного маршрутизатора універсальний комп'ютер з декількома мережевими картами і програмним забезпеченням з функціями протоколів маршрутизації.

8. Кваліфікація персоналу компанії і їх переваги.

Адміністрування мережі і рівень її складності, дуже залежить від типу мережеских протоколів, які будуть використовуватися в мережі. Важливо враховувати наявність досвіду адміністратора мережі в налаштуванні і впровадженні цих протоколів в мережу.

2.3 Аналіз використання протоколів динамічної маршрутизації

З метою вибору кращого протоколу маршрутизації по поставленому завданню про забезпечення і підвищення надійності мережі, необхідно враховувати їх недоліки та переваги.

Протоколи маршрутизації діляться на два основні класи: протоколи внутрішніх шлюзів (Interior Gateway Protocols - IGP) і протоколи зовнішніх шлюзів (Exterior Gateway Protocols - EGP). Протоколи класу IGP проектувалися для обміну інформацією про мережах і підсетях між внутрішніми маршрутизаторами однієї автономної системи (Autonomous System - AS), тобто між маршрутизаторами, що знаходяться під єдиним адміністративним керуванням, і використовують один протокол маршрутизації. Такими мережами

можуть бути мережі провайдерів послуг Internet, великих урядових і науково-дослідних організацій, приватних комерційних концернів. Протоколи EGP проектувалися для обміну маршрутною інформацією між прикордонними маршрутизаторами різних автономних систем. Домінуючим EGP-протоколом сьогодні є протокол граничної маршрутизації версії 4 (Border Gateway Protocol version 4 - BGP-4). Цей протокол використовується для обміну маршрутною інформацією між AS мережі Internet. За методом поширення маршрутної інформації протоколи IGP діляться на дистанційно-векторні і стану каналів зв'язку. У методі вектора відстаней кожен маршрутизатор через рівні проміжки часу посилає сусіднім маршрутизаторам оновлення всієї або частини своєї таблиці маршрутизації.

У міру поширення маршрутної інформації в мережі кожен маршрутизатор може обчислити відстані від нього до всіх мереж і підмереж в межах внутрішньокорпоративної мережі. Найбільш поширеними протоколами даного типу є RIP (Routing Information Protocol) і IGRP (Interior Gateway Routing Protocol). У методі обліку стану каналів зв'язку кожен маршрутизатор корпоративної мережі посилає іншим маршрутизаторів інформацію про своїх безпосередніх з'єднаннях з мережами і маршрутизаторами. На основі отриманої інформації про всі локальних судинних в мережі, кожен маршрутизатор здатний побудувати її повний топологічний граф, а потім заповнити свою таблицю, використовуючи складний алгоритм вибору першого найкоротшого шляху (Shortest Path First - SPF). Найбільш відомими протоколами даного типу є OSPF (Open Shortest Path First) і IS-IS (Intermediate System to Intermediate System). Існують також гібридні протоколи, що поєднують в собі переваги обох методів поширення маршрутної інформації. Прикладом гібридного протоколу є EIGRP (Enhanced Interior Gateway Routing Protocol).

Протоколи, засновані на методі вектора відстані, вимагають менше обчислювальних ресурсів маршрутизатора, ніж протоколи з вибором станом каналів зв'язку з їх складними SPF-алгоритмами. З іншого боку, протоколи з вибором станом каналів зв'язку займають меншу частину смуги пропускання

мережі (крім початкового етапу вивчення топології мережі) так, як вони поширюють тільки інформацію про зміни, а не всю таблицю маршрутизації, що особливо важливо для великих мереж.

В якості інших критеріїв порівняння протоколів динамічної маршрутизації можна виділити наступні.

1. Швидкість збіжності.

Ця характеристика протоколу визначає тривалість тимчасового інтервалу можливої нестабільної роботи мережі, в перебігу якого протокол виявляє недоступний маршрут, вибирає новий маршрут і поширює нову інформацію по мережі. Швидкість реакції на зміни в мережевий топології особливо важлива при підтримці важливих додатків, що вимагають високого ступеня готовності мережі. Протоколи, засновані на методі вектора відстані, вимагають більшого часу для збіжності, ніж протоколи з вибором станом каналу зв'язку, тому що інформація про новий шляху передається від одного маршрутизатора до іншого побічно без вказівки джерела її походження в процесі періодичних розсилок.

2. Можливість обліку в метриці (критерії) вибору найбільш раціонального маршруту різних характеристик маршруту.

Метрика розраховується на основі однієї або кількох характеристик шляху. До найбільш вживаною характеристикам шляху відносяться: кількість переходів (проміжних маршрутизаторів в дорозі); пропускна здатність каналів зв'язку; затримка пакета в дорозі; надійність (частота виникнення помилок каналах зв'язку); навантаження (завантаженість маршрутизаторів і каналів зв'язку); вартість (довільне значення, яка призначається адміністратором на підставу як перерахованих вище, так і інших міркувань, наприклад фінансових). Метрики, що обчислюються на основі декількох показників, забезпечують більшу гнучкість при виборі маршруту. Можливості протоколу підтримувати одночасно кілька метрик дозволяють задовольняти вимоги QoS-трафіку (Quality of Service) різних додатків.

3. Можливість балансування навантаження між декількома маршрутами.

Можливість зберігання в таблицях маршрутизації декількох маршрутів до однієї мережі (з рівними або навіть відрізняються метриками) дає можливість маршрутизатора знижувати завантаження ліній зв'язку, шляхом поперемінної відсилання пакетів по кожному з маршрутів. Слід звернути увагу на те, що балансування навантаження може викликати проблеми в тих випадках, коли додаток використовує дейтаграмний протоколи канального і транспортного рівнів, що не нумерують і, отже, не відновлюють порядок проходження пакетів, як це робить, наприклад, транспортний протокол зі установленням з'єднання ТСП.

4. Можливість об'єднання маршрутів на співпадаючих ділянках.

Наявність даної функції сприяє зниженню відносної складності великої мережі, скорочення кількості записів в таблицях маршрутизаторів і прискоренню пошуку в них. Об'єднання маршрутів вимагає, щоб протокол маршрутизації підтримував маски підмереж змінної довжини і був здатний поширювати інформацію про мережеві маски разом з інформацією про мережевих маршрутах.

5. Максимальна кількість маршрутизаторів в мережі визначає можливості її масштабування.

Це обмеження побічно пов'язане з іншими характеристиками протоколу маршрутизації, що впливають на його здатність працювати у великій мережі (наприклад, швидкістю збіжності, часткою смуги пропускання мережі, необхідної для передачі службових повідомлень протоколу).

6. Необхідність попередньої логічної підготовки мережі.

Деякі протоколи маршрутизації для досягнення відповідного рівня масштабування (зменшення споживання обчислювальних ресурсів маршрутизаторів і пропускної здатності мережі) мають на увазі виділення в мережі логічних областей і зв'язків між ними. впровадження таких протоколів може зажадати серйозної інженерної проробки проекту мережі (її топології та схеми адресації).

7. Забезпечення безпеки при обміні маршрутною інформацією.

Якщо мережа підтримує обмін маршрутною інформацією між підмережами, з'єднаними глобальними зв'язками, то потрапляння такої інформації в руки зломисників може становити загрозу безпеці мережі. У таких випадках підтримка протоколом маршрутизації методів аутентифікації джерела і шифрування маршрутної інформації набуває важливого значення.

8. Доступність програмного забезпечення (ПО) реалізації протоколу маршрутизації.

Проколи можуть бути відритими і підтримуватися різними виробниками апаратних маршрутизаторів і ПО для універсальних комп'ютерів, а можуть бути закритими і реалізуватися лише певними компаніями.

9. Перспективність - реалізація в протоколі перспективних можливостей (наприклад, протоколу IP6, підтримка трафік інжинірингу).

2.4 Висновки до розділу 2

В даному розділі було розглянуто, що таке маршрутизація і яку роль вона виконує в мережі. Було обґрунтовано, які основні принципи маршрутизації, використовує маршрутизатор для передачі трафіку по мережі, а саме:

Маршрутизатор будує таблицю маршрутизації на підставі інформації, отриманої через свої інтерфейси, від сусідніх маршрутизаторів. Це здійснюється за допомогою протоколу динамічної маршрутизації, який відправляє всім сусідам повідомлення про те, що маршрут змінився або в даний момент недоступний.

Маршрутизатор це пристрій, який приймає рішення про передачу пакета, ґрунтуючись лише на інформації, яка міститься в його таблиці маршрутизації. Тобто, якщо усі мережеві елементи які знаходяться в одному мережевому домені, та не встигнуть змінити свою таблицю маршрутизації, пакет може бути не доставлений до точки призначення.

В рамках дослідження впливу протоколів маршрутизації на надійність телекомунікаційної мережі, пропонується метод нарощування надмірності мережі за допомогою резервних шляхів, шляхом штучного введення їх в мережу та

віртуальних логічних каналів, які будуть утворені при використанні додаткових мережевих технологій. Трафік, який буде передаватися до місця призначення, зможе бути переданий і доставлений через різні шляхи. Також, було приведено короткий приклад маршрутної таблиці маршрутизатора для первісного ознайомлення та уявлення, як будується маршрут в мережі.

У розділі розповідається про вимоги мережі до протоколу маршрутизації для повноцінного розуміння при виборі протоколу маршрутизації та введенням його в експлуатацію з якісною працездатністю в мережі. Основними вимогами при виборі протоколу маршрутизації, вважається:

1. Топологія і складність мережі.
2. Розміри мережі і необхідність в її подальшому масштабуванні.
3. Завантаженість мережі.
4. Вимоги до надійності мережі.
5. Вимоги до захисту інформації в мережі.
6. Необхідність підключення маршрутизації сегмента до вже існуючої мережі.
7. Можливість організації програмних маршрутизаторів.
8. Кваліфікація і суб'єктивні переваги обслуговуючого персоналу.

Також, було надано короткий порівняльний аналіз о протоколах динамічної маршрутизації, а саме дистанційно-векторних протоколів і протоколів за станом каналу. В якості основних критеріїв порівняння протоколів динамічної маршрутизації, було виділено наступні критерії:

1. Швидкість збіжності.
2. Можливість обліку в метриці (критерії) вибору найбільш раціонального маршруту різних характеристик маршруту.
3. Можливість балансування навантаження між декількома маршрутами.
4. Можливість об'єднання маршрутів на співпадаючих ділянках.
5. Максимальна кількість маршрутизаторів в мережі визначає можливості її масштабування.
6. Необхідність попередньої логічної підготовки мережі.
7. Забезпечення безпеки при обміні маршрутною інформацією.

8. Доступність програмного забезпечення (ПО) реалізації протоколу маршрутизації.
9. Перспективність - реалізація в протоколі перспективних можливостей (наприклад, протоколу IP6, підтримка трафік інжинірингу).

У наступному розділі буде розглянуто більш детально про можливості і функції протоколів динамічної маршрутизації, їх недоліки та переваги.

3 АНАЛІЗ ЗАСТОСУВАННЯ ДИНАМІЧНИХ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В СИСТЕМАХ ДЛЯ ПІДВИЩЕННЯ ТА ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ МЕРЕЖІ

3.1 Аналіз використання дистанційно-векторних протоколів маршрутизації

Алгоритм дистанційно-векторної маршрутизації визначає напрямок (вектор) і відстань (лічильник вузлів) для кожного з каналів зв'язку, що утворюють мережу.

При використанні цього алгоритму маршрутизатор періодично (наприклад, кожні 30 секунд) пересилає всю або частину своєї таблиці маршрутизації своїм сусідам.

Періодичні поновлення розсилаються маршрутизатором, що використовують дистанційно векторний алгоритм, навіть якщо не відбулися ніякі зміни в мережі. Отримавши таблицю маршрутизації від свого сусіда, маршрутизатор може перевірити вже відомі маршрути і внести необхідні зміни на основі отриманого поновлення. Такий процес іноді називають " маршрутизацією за чутками ", оскільки уявлення маршрутизатора про структуру мережі базується на даних його сусідів. Дистанційно-векторні протоколи маршрутизації засновані на алгоритмі Беллмана Форда (Bellman Ford) і використовують його для пошуку найкращого маршруту.

Дистанційно векторний алгоритм є основою для наступних протоколів:

- для протоколу маршрутної інформації (Routing Information Protocol RIP)
- одного з найбільш широко поширених протоколів IGP типу, що використовує в якості метрики лічильник вузлів;
- для протоколу маршрутизації внутрішнього шлюзу (Interior Gateway Routing Protocol IGRP); корпорація Cisco розробила цей протокол для маршрутизації в великих гетерогенних мережах;
- для вдосконаленого протоколу маршрутизації внутрішнього шлюзу (Enhanced Interior Gateway Routing Protocol EIGRP), що представляє собою поліпшену версію IGRP від корпорації Cisco; цей протокол має виключно швидку

конвергенцію, працює значно ефективніше, ніж його попередник, і поєднує в собі всі переваги дистанційно векторних алгоритмів і протоколів з урахуванням стану каналів.

3.1.1 Протокол RIP

Протокол RIP використовує дистанційно-векторний алгоритм і в більшості випадків, використовує для маршрутизації найпростішу метрику - кількість проміжних вузлів до мережі призначення.

Перевагою протоколу RIP, є легкість його налаштування, яка не вимагає особливої кваліфікації в адмініструванні. Протокол маршрутної інформації (Routing Information Protocol - RIP) використовує лічильник кількості транзитних вузлів для визначення напрямку і відстані для будь-якого з каналів мережі.

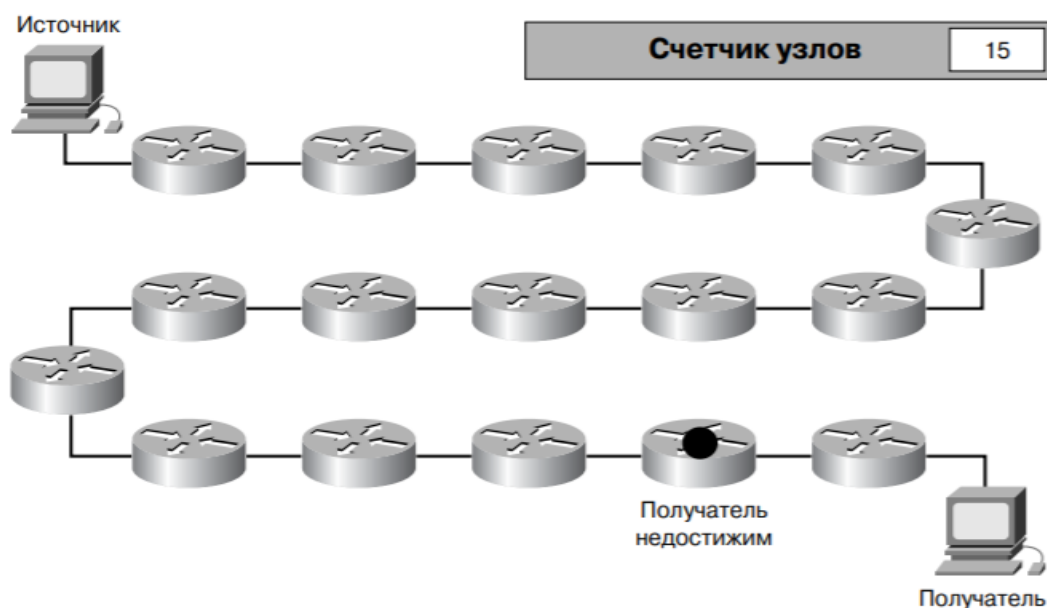


Рисунок 3.1 Протокол RIP використовує в якості метрики лічильник транзитних вузлів

Якщо існують декілька маршрутів до одержувача, протокол RIP вибере той з них, який має найменше значення лічильника транзитних вузлів. Оскільки лічильник є єдиною метрикою, використовуваною протоколом RIP, обраний

маршрут далеко не завжди виявляється найкоротшим. Протокол RIP версії 1 дозволяє використовувати тільки класову (classfull) маршрутизацію. Це означає, що всі мережеві пристрої повинні мати однакову маску мережі, оскільки RIP версії 1 не включає в маршрутні поновлення інформацію про неї.

Протокол RIP версії 2 використовує так звану префіксну маршрутизацію (prefix routing) і пересилає маску мережі разом з анонсами таблиць маршрутизації: саме за рахунок цієї функції забезпечується підтримка безкласової маршрутизації. Завдяки протоколам безкласової маршрутизації можна використовувати підмережі з різної довжини масками всередині однієї і тієї ж мережі. Використання масок підмережі різної довжини всередині однієї мережі називається технологією масок змінної довжини (Variable Length Subnet Mask - VLSM).

3.1.2 Протокол IGRP

Закритий дистанційно-векторний протокол IGRP компанії Cisco Systems був спроектований для усунення ряду недоліків протоколу RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з відмінними характеристиками смуги пропускання і величини затримки.

Протокол використовує комбіновану метрику, яка включає затримку, смугу пропускання, надійність і завантаженість маршруту. Вагові коефіцієнти, що визначають внесок цих характеристик в результуючу метрику, задаються користувачем, забезпечуючи гнучку адаптацію до його конкретним завданням. Показники затримки і смуги пропускання конфігуруються для кожної лінії зв'язку попередньо, а показники надійності і завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі.

Для підтримки вимог QOS різних додатків можна підготувати кілька маршрутних таблиць, побудованих на основі метрик з різними значеннями вагових коефіцієнтів.

Протокол IGRP забезпечує швидшу збіжність, ніж RIP завдяки застосуванню пакетів оновлення з миттєвою розсилкою (інформація про зміни в мережі відправляється відразу, як тільки стає доступною, не чекаючи чергового часу поновлення). Протокол підтримує балансування навантаження між декількома маршрутами навіть в тому випадку, якщо їх метрики не рівні, але знаходяться в межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів відправлених по кожній колії даних буде пропорційно співвідношенню їх метрик.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини і можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні кошти аутентифікації при обміні маршрутною інформацією. Непрямим засобом захисту є можливість прийому повідомлень про оновлення маршрутів тільки від тих маршрутизаторів, які даний визначає як «сусідні», а також можливість внесення змін в конфігурацію маршрутизатора тільки на підставі пароля, який зберігається в зашифрованому вигляді.

3.1.3 Протокол EIGRP

Протокол EIGRP компанії Cisco Systems є поліпшену версію вихідного протоколу IGRP. Протокол є гібридним і заснований на алгоритмі поновлення Diffusing-Update Algorithm (DUAL). Він поєднує в собі кращі сторони дистанційно-векторних протоколів (простота алгоритму вибору оптимального маршруту) і протоколів стану каналів зв'язку (швидка збіжність і економія смуги пропускання мережі за рахунок повідомлень тільки про стан зв'язків і про їх зміну). Усі розсилки протоколу є мультікастними або індивідуальними. Таким чином, інформація розсилається тільки при змінах і тільки тим маршрутизаторам, яких вона стосується.

З метою підвищення масштабованості протоколу в нього додана підтримка масок підмереж змінної довжини і можливість об'єднання маршрутів. Маршрути діляться на внутрішні і зовнішні - отримані від інших протоколів маршрутизації або записані в таблиці статично.

В останніх версіях EIGRP є засоби захисту, що не дозволяють зловмисникам дописувати елементи в таблицю маршрутизації, і аутентифікація по ключу MD5. Крім того, в даний час для EIGRP розробляють засоби підтримки IPv6, так що цей протокол буде розвиватися надалі. Основним недоліком EIGRP, як і його попередника, є закритість і реалізація тільки на обладнанні Cisco Systems. Протокол добре сумісний з IGRP, а також з RIP.

3.1.4 Протокол BGP

Протокол граничного шлюзу (Border Gateway Protocol - BGP) є прикладом протоколу EGP типу. Протокол BGP розроблявся як зовнішній для організації маршрутизації між автономними системами в глобальній мережі Internet (максимальне число маршрутизаторів 65534 між AS). В даний час в Internet використовується 4-я версія протоколу BGP-4. Хоча протокол відноситься до зовнішніх протоколів маршрутизації, його іноді застосовують і для внутрішньої маршрутизації.

BGP є протоколом, що орієнтується на вектор відстані. Однак, на відміну від RIP і IGRP протокол BGP не вимагає періодичного оновлення всієї маршрутної таблиці. Обмін повними таблицями виконується між маршрутизаторами тільки при їх початковому підключенні. Надалі відсилаються тільки повідомлення про оновлення в таблицях, причому тільки тим маршрутизаторам, які явно вказані в якості сусідніх. В одному оновленні BGP-4 може бути оголошено про одне новий маршрут або анулювання декількох перестали існувати. Все це сприяє зниженню службового трафіку.

Метрика BGP є довільне число одиниць, що характеризує ступінь переваги конкретного маршруту, і встановлюються адміністратором мережі, в основному

виходячи з міркувань договірних і фінансових переваг, можливо, з обліку інших факторів (за замовчуванням на підставі мінімального числа проміжних AS).

У різних маршрутизаторів може використовуватися різна маршрутна політика. Хоча BGP підтримує маршрутну таблицю всіх можливих шляхів до конкретної мережі, в своїх повідомленнях про коригування він оголошує тільки про оптимальні маршрути. Наявність в таблиці альтернативних маршрутів прискорює реакцію маршрутизатора на інформацію про недосяжність основного шляху, а також дозволяє підтримувати балансування навантаження. Оскільки протокол орієнтований на обмін даними між різними AS, де при виборі маршрутів переважають, як правило, не технічні, а політичні міркування, то процес балансування навантаження на увазі осмислене розподіл маршрутів між альтернативними каналами за допомогою настройки відповідних параметрів протоколу.

Повідомлення BGP-4 про коригування містять послідовність AS, через які може бути досягнута зазначена мережа, її IP-адреса та довжина маски префікса (підтримується тільки безкласовість адресація CIDR). Протокол дозволяє об'єднувати маршрути. Перелік AS використовується для поліпшення збіжності, швидкість якої у протоколу не висока. Для забезпечення безпеки можуть застосовуватися різні способи аутентифікації маршрутизаторів. Протокол сумісний з RIP і OSPF.

3.2 Аналіз використання протоколів маршрутизації за станом каналів

Протоколи маршрутизації, що використовують алгоритм з урахуванням стану каналів, були розроблені для подолання обмежень, пов'язаних з використанням дистанційно-векторних протоколів. Алгоритм з урахуванням стану каналу дає можливість протоколам швидко реагувати на зміни мережі, розсилати оновлення тільки в разі появи змін і розсилати періодичні оновлення (Звані оновленнями стану каналу) через великі проміжки часу, приблизно один раз кожні 30 хвилин.

Коли стан каналу змінюється, пристрій, яке виявило таку зміну, формує повідомлення про стан каналу (Link State Advertisement - LSA), що відноситься до цього каналу (маршруту), і розсилає його всім сусіднім маршрутизаторам. Кожен маршрутизатор отримує копію повідомлення про стан каналу і на цій підставі оновлює свою базу стану каналів (топологічну базу), після чого пересилає копію повідомлення всім своїм сусідам. Така масова розсилка сповіщення потрібна, щоб гарантувати, що всі маршрутизатори оновлять свої бази даних і створять оновлену таблицю маршрутизації, яка відображає нову топологію.

База даних стану каналу використовується для виявлення найкращого мережевого шляху. Маршрутизація з урахуванням стану каналу заснована на алгоритмі першочергового визначення найкоротшого маршруту (Shortest Path First - SPF) Дейкстра (Dijkstra) для побудови SPF дерева, на основі якого приймається рішення про те, який маршрут є найкращим. Найкращий (найкоротший) маршрут вибирається з дерева першочергового визначення найкоротшого маршруту і поміщається в таблицю маршрутизації.

Прикладами протоколів, що використовують алгоритм з урахуванням стану каналів, є OSPF і IS-IS.

3.2.1 Протокол OSPF

Відкритий протокол пошуку найкоротшого шляху (Open Shortest Path First OSPF) використовує алгоритм маршрутизації станом каналів.

Найбільш універсальним і гнучким у налаштуванні протоколом динамічної маршрутизації в корпоративних мережах на сьогоднішній день є відкритий протокол вибору першого найкоротшого шляху (Open Shortest Path First Protocol - OSPF).

Протокол спочатку був орієнтований на роботу в великих мережах (до 65536 маршрутизаторів) зі складною топологією. Він заснований на алгоритмі стану каналів зв'язку і має високу стійкість до змін топології мережі і швидкої

збіжністю. При виборі маршруту використовується метрика пропускної здатності складовою мережі (тобто передача даних по найбільш швидкісних каналів зв'язку). Протокол може підтримувати різні вимоги IP-пакетів на якість обслуговування (пропускна здатність, затримка і надійність) за допомогою побудови окремої таблиці маршрутизації для кожного з цих показників.

Протокол володіє і іншими достоїнствами, корисними в великих сучасних мережах. До них відносяться можливість балансування навантаження між каналами з рівними метриками і засоби аутентифікації як по нешифрований пароллю, так і по шифрованому (шляхом додавання до пакету дайджесту ключа і тіла пакета за алгоритмом MD5). нумерація пакетів виключає їх повторюваність і таким чином можливість повторної атаки. Відкритість протоколу визначає його підтримку практично всіма виробниками мережевого устаткування, реалізації в ПО під всі популярні ОС (наприклад, для Unix-подібних ОС - пакети Zebra, Quagga і ін.), а також безпосередню інтеграцію в ряд ОС (наприклад, Windows 2000 Server і вище, OpenBSD, Cisco IOS, Solaris 10 і т.д.).

До недоліків проколу слід віднести високу обчислювальну складність і, отже, високі вимоги, що пред'являються до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає зі збільшенням розмірів мережі. Тому для збільшення масштабованості протоколу застосовується поділ мережі на логічні області, з'єднані магістральною областю. Внутрішня топологічна інформація між областями не віддається. Скорочення обсягів таблиць маршрутизації і зниження службового трафіку при оновленні топологічної інформації служить можливість об'єднання декількох адрес мереж в один при виявленні у них загального префікса, і заміна ширококомовних розсилок мультікастинговими. З метою економії IP-адрес в з'єднаннях типу «точка - точка» між маршрутизаторами призначати кінцевим точкам адреси не обов'язково. Платою за ці переваги є складність конфігурації і необхідність ретельного попереднього планування мережі для її оптимальної роботи (розбивка на області, виділення магістралі, розподіл функцій між маршрутизаторами з урахуванням їх обчислювальної потужності: рядові, виділені в зоні, прикордонні і т.д.).

В якості перспективних функцій OSPF слід назвати підтримку протоколу Ipv6 і можливість вибору маршруту на підставі поточного коефіцієнта завантаженості каналів зв'язку (розширена версія OSPF отримала назву Constrained Shortest Path First - CSPF).

3.2.2 Протокол IS-IS

Протокол обміну маршрутною інформацією між проміжними системами (Intermediate System to Intermediate System IS-IS) використовує алгоритм маршрутизації станом каналу для стека протоколів моделі OSI. Він поширює маршрутну інформацію для протоколу мережевого обслуговування (Connectionless Network Protocol - CLNP), для відповідних ISO служб мережевого обслуговування без встановлення з'єднання (Connectionless Network Service - CLNS).

Інтегрований протокол IS-IS є варіантом реалізації протоколу IS-IS для маршрутизації декількох мережевих протоколів. Інтегрований протокол IS-IS об'єднує CLNP маршрути з інформацією про IP мережах і масках підмереж. Завдяки поєднанню ISO CLNS і IP маршрутизації в одному протоколі інтегрований протокол IS-IS надає альтернативу протоколу OSPF при використанні в IP мережах.

В даний час цей протокол дуже рідко використовується в корпоративних мережах. Це викликано повною перевагою над ним протоколу OSPF, який, по суті, є вдосконаленим IS-IS. До недоліків протоколу відноситься його нездатність підтримувати маски підмереж змінної довжини, об'єднувати маршрути, а також широкомовний характер розсилок сусіднім маршрутизаторам. Все це негативно впливає на швидкість збіжності, навантаження маршрутизаторів і завантаженість ліній зв'язку.

3.3 Аналіз застосування додаткових мережевих технологій для підвищення надійності мережі

Ефективним засобом захисту від збоїв служить побудова відмовостійких рішень. Особливо це актуально там, де найменший простий може обернутися серйозними втратами. Щоб такого не сталося, були розроблені спеціальні протоколи: всім відомий STP, різноманітні протоколи агрегації каналів, протоколи, що забезпечують відмовостійкість шлюзу. Однак, концентруючись на цю властивість, дуже часто не беруть до уваги безпеку.

Відмовостійкість - це властивість технічної системи зберігати свою працездатність після відмови одного або декількох складових компонентів. Уяви ситуацію, коли з мережі існує один-єдиний вихід у зовнішній світ і цей вихід є шлюзом за замовчуванням. Тоді в разі його падіння вже ніщо не допоможе - неважливо буде, наскільки якісно спроектована мережа, клієнти просто не зможуть вийти за межі своєї підмережі. Саме такі проблеми і покликані вирішувати протоколи відмовостійкості. Але у них є свої нюанси, які можуть стати серйозною загрозою для безпеки системи.

3.3.1 Протокол HSRP

Hot Standby Router Protocol (HSRP) є Cisco власний протокол резервування для створення відмовостійкої шлюзу. Протокол встановлює зв'язок між шлюзами для досягнення за замовчуванням відновлення після збою шлюзу, якщо основний шлюз стає недоступним. HSRP шлюз відправки многоадресного вітання повідомлення іншим шлюзів, щоб повідомити їх про свої пріоритети (що є кращим шлюзом) і поточний статус (активний або резервний).

Первинний маршрутизатор з найвищим пріоритетом виступатиме в якості віртуального маршрутизатора з наперед визначеним IP - адреса шлюзу, і буде реагувати на ARP або ND запит від машин, підключених до локальної мережі за допомогою віртуального адреси MAC. Якщо основний маршрутизатор повинен зазнати невдачі, маршрутизатор з наступного найвищим пріоритетом буде взяти на себе IP - адреса шлюзу і відповідати на ARP - запити з тим же MAC - адреса, що дозволить досягти прозорого шлюзу перехід на інший ресурс.

HSRP має можливість ініціювати перехід на інший ресурс, якщо один або декілька інтерфейсів маршрутизатора знизитися. Це може бути корисно для двох філій маршрутизаторів кожного з одним зв'язком назад до шлюзу. Якщо посилення первинного маршрутизатора йде вниз, резервний маршрутизатор візьме на себе основні функціональні можливості і, таким чином, зберегти підключення до шлюзу.

Проте справи з безпекою HSRP йдуть не так вже й погано. Існує можливість використовувати MD5-хешування. MD5-хеш обчислюється в кожному HSRP-пакеті, і секретний ключ відомий тільки легітимним учасникам групи HSRP. Рядок з MD5-хешем відправляється в кожному пакеті; як тільки пакет отриманий, учасники перераховують хеш, і якщо значення збігається, то повідомлення приймається. Складність проведення атаки в таких умовах в тому, що хеш використовується не в якості ключа, а для перевірки справжності повідомлення.

3.3.2 Протокол ECMP

Протокол Equal-Cost Multi-Path (ECMP) описаний в стандарті IETF RFC-2992. ECMP працює спільно з протоколами маршрутизації, такими як RIP і OSPF, і дозволяє встановити кілька рівноцінних маршрутів для передачі даних.

ECMP може працювати спільно з такими протоколами маршрутизації як RIP, OSPF і BGP для визначення вартостей маршрутів і пошуку маршрутів з однаковою вартістю, які можуть бути використані для розподілу навантаження і оптимізації пропускної здатності мережі. Дані можуть одночасно передаватися не більш ніж по 4-м маршрутами, але якщо ECMP використовується спільно з MLT, то кількість фізичних каналів для передачі даних збільшується, так як кожне MLT з'єднання налаштовується як один ECMP маршрут.

При використанні ECMP в таблиці маршрутизації відображається до 4-х маршрутів до даної мережі, ці маршрути позначаються літерою "E", як маршрути ECMP. Використання протоколів маршрутизації без ECMP і використання їх же спільно з ECMP можна приблизно порівняти з використанням Spanning Tree

проти використання MLT, якщо розглядати пропускну здатність мережі. З точки зору відмовостійкості, ESMР також як і MLT, забезпечує відновлення за частки секунди. Це потрібно для того, щоб передані дані не губилися в транзитній мережі.

При проектуванні мережі, особливо центральної або магістральної її частини, деякі вважають за краще використовувати комутацію на рівні 2 (відповідно до моделі OSI), і, відповідно, MLT і SMLT, а інші маршрутизацію і ESMР. Вибір залежить від необхідності використання VLAN, члени якого знаходяться по всій мережі. Також в разі з'єднання мереж через прозору мережу Ethernet (наприклад, мережа Metro Ethernet), важливо бути впевненим, що включено наскрізне визначення відмов, або необхідно використовувати маршрутизацію.

3.3.3 Протокол SNMP

SNMP (англ. Simple Network Management Protocol - простий протокол мережевого управління) - стандартний інтернет-протокол для управління пристроями в IP-мережах на основі архітектур TCP / UDP. До підтримуючих SNMP пристроїв відносяться маршрутизатори, комутатори, сервери, робочі станції, принтери, модемні стійки і інші.

При використанні SNMP один або більше адміністративних комп'ютерів (де функціонують програмні засоби, звані менеджерами) виконують відстеження або управління групою хостів або пристроїв в комп'ютерній мережі. На кожній керованій системі є постійно запущена програма, яка називається агент, яка через SNMP передає інформацію менеджеру.

Керовані протоколом SNMP мережі складаються з трьох ключових компонентів:

- Керована пристрій;

- Агент - програмне забезпечення, що запускається на керованому пристрої, або на пристрої, підключеному до інтерфейсу управління керованого пристрою;
- Система мережевого управління (Network Management System, NMS) - програмне забезпечення, яке взаємодіє з менеджерами для підтримки комплексної структури даних, що відбиває стан мережі.

Керований пристрій - елемент мережі (обладнання або програмний засіб), який реалізує інтерфейс управління (не обов'язково SNMP), який дозволяє односпрямований (тільки для читання) або двонаправлений доступ до конкретної інформації про елемент. Керовані пристрої обмінюються цією інформацією з менеджером. Керовані пристрої можуть ставитися до будь-якого виду пристроїв: маршрутизатори, сервери доступу, комутатори, мости, концентратори, IP-телефони, IP-відеокамери, комп'ютери-хости, принтери і т.п.

Агентом називається програмний модуль мережевого управління, що розташовується на керованому пристрої, або на пристрої, підключеному до інтерфейсу управління керованого пристрою. Агент має локальним знанням керуючої інформації і переводить цю інформацію в специфічну для SNMP форму або з неї (медіація даних).

До складу Системи мережевого управління (NMS) входить додаток, що відстежує і контролює керовані пристрої. NMS забезпечують основну частину обробки даних, необхідних для мережевого управління. У будь-якій керованій мережі може бути одна і більше NMS.

3.3.4 Протокол VRRP

VRRP (Virtual Router Redundancy Protocol) - мережевий протокол, призначений для збільшення доступності маршрутизаторів, що виконують роль шлюзу. Це досягається шляхом об'єднання групи маршрутизаторів в один віртуальний маршрутизатор і призначення їм загальної IP-адреси, який і буде використовуватися як шлюз для комп'ютерів в мережі. Протокол VRRP

призначений для збільшення доступності маршрутизаторів, які виконують роль шлюзу.

Для групи маршрутизаторів налаштовується їх приналежність віртуальному маршрутизатора. Фактично, віртуальний маршрутизатор - це група інтерфейсів маршрутизаторів, які знаходяться в одній мережі і розділяють Virtual Router Identifier (VRID) і віртуальний IP-адреса.

VRRP-маршрутизатор може перебувати в кількох віртуальних маршрутизаторах, кожен з унікальною комбінацією VRID / IP-адреса. Відповідності між VRID і IP-адресою повинні бути однаковими на всіх маршрутизаторах в одній мережі.

У будь-який момент часу тільки один з фізичних маршрутизаторів виконує маршрутизацію трафіку, тобто стає VRRP Master router, інші маршрутизатори в групі стають VRRP Backup router. Якщо поточний VRRP Master router стає недоступним, то його роль бере на себе один з VRRP Backup маршрутизаторів, той у якого найвищий пріоритет. Завдання пріоритету дозволяє визначити більш пріоритетні шляхи адміністративно.

Backup-маршрутизатор не буде намагатися перехопити на себе роль Master-маршрутизатора, якщо тільки у нього не вищий пріоритет, ніж у поточного Master-маршрутизатора. VRRP дозволяє адміністративно заборонити перехоплення ролі Master-маршрутизатора. Єдиний виняток з цього правила - VRRP-маршрутизатор завжди буде ставати Master, якщо він власник IP-адреси, який присвоєно віртуальному маршрутизатора.

У кожному віртуальному маршрутизаторі тільки Master відправляє періодичні VRRP-оголошення на зарезервований груповий адресу 224.0.0.18. На каналному рівні в якості MAC-адреси відправника VRRP-оголошень використовується віртуальний MAC-адресу.

3.3.5 Протокол GLBP

GLBP (Gateway Load Balancing Protocol) - пропрієтарний протокол Cisco, призначений для збільшення доступності маршрутизаторів виконують роль шлюзу і балансування навантаження між цими маршрутизаторами.

GLBP працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, такими як HSRP і VRRP. Ці протоколи дозволяють декільком маршрутизаторів брати участь в сконфігурованій віртуальній групі маршрутизаторів із загальним віртуальним IP-адресою. Один член групи вибирається активним маршрутизатором, в той час як інші залишаються неактивними до тих пір, поки не відбудеться збій з активним маршрутизатором. При цьому ці резервні маршрутизатори мають ресурсами, які майже не використовуються протягом всього часу експлуатації цієї системи. GLBP забезпечує розподіл навантаження на декілька маршрутизаторів (шлюзів) використовуючи один віртуальний IP-адреса і кілька віртуальних MAC-адрес. Кожен хост налаштований з однаковим віртуальним IP-адресою і все маршрутизатори у віртуальній групі беруть участь в передачі пакетів.

Члени GLBP групи вибирають один шлюз який буде активним віртуальним шлюзом active virtual gateway (AVG) для цієї групи. Інші члени групи забезпечують резервування для AVG в разі якщо AVG стане недоступним. AVG призначає віртуальний MAC адреса для кожного члена GLBP групи. Кожен член групи бере участь в передачі пакетів, використовуючи віртуальний MAC адресу, виданий AVG. Цих членів групи називають active virtual forwarders (AVFs). AVG відповідальний за видачу відповідей по протоколу Address Resolution Protocol (ARP) на запити до віртуального IP-адресою. Розподіл навантаження досягається тим що AVG відповідає на ARP запити використовуючи різні віртуальні MAC-адреси.

GLBP Gateway Priority визначає роль, яку кожен маршрутизатор AVF грає в групі. Тобто за допомогою цієї властивості можна визначити послідовність вибору нового AVG, якщо старий AVG стане недоступним. Пріоритет можна

визначити на кожному маршрутизаторі значенням від 1 до 255 командою: `glbr priority`. Маршрутизатор з великим пріоритетом стає AVG. За замовчуванням схема вибору AVG тільки на основі пріоритету вимкнена. Запасний AVF стане AVG тільки якщо поточний AVG стане недоступним.

3.4 Висновки до розділу 3

У цьому розділі було обґрунтовано класифікацію протоколів маршрутизації, які діляться на два типи: дистанційно-векторні та за станом каналу. Серед широко відомих протоколів маршрутизації, розглядалися: RIP, IGRP, EIGRP, BGP, OSPF, IS-IS. Серед вищезазначених протоколів динамічної маршрутизації, кращими протоколами за показником збіжності і масштабованості, вважаються протоколи OSPF, EIGRP та IS-IS. Протоколи IS-IS і протокол EIGRP, вважаються пропрієтарними протоколами, тому впроваджувати їх в мережу, є не зовсім доцільним завданням, так як в більшості телекомунікаційних мережах, вони не зможуть просто виконувати свої функції.

Протокол BGP використовується для зв'язку з різними автономними системами, в даному дослідженні, він не використовується, так як дане дослідження щодо впливу протоколів маршрутизації на надійність телекомунікаційної мережі, проводиться всередині мережі без застосування зв'язку з іншими глобальними мережами.

Протокол RIP вже довгий час майже ніде не використовується, так як рівень його масштабованості дуже обмежений, але для порівняльного аналізу в дослідженнях, був обраний протокол RIP, щоб перевірити наскільки відрізняється час збіжності в мережі у порівнянні з іншими протоколами і чи здатний протокол RIP, підвищити надійність мережі.

Протокол IGRP вважається старою версією протоколу EIGRP. Даний протокол використовується для маршрутизації трафіку, всередині однієї автономної системи. У протоколі RIP, метрикою, виступало кількість проміжних вузлів до мережі призначення. У протоколі IGRP все набагато цікавіше, в ньому

використовується композитна метрика, що обчислюється на основі ширини смуги пропускання, затримки, рівня завантаження каналу і надійності каналу. Тому, в рамках другого дослідження, був обраний протокол IGRP, як більш простий протокол динамічної маршрутизації, але з більш широкою комбінованою метрикою і часом збіжності вузлів.

Для третього дослідження, було обрано протокол OSPF, який на даний момент, є кращим рішенням серед рівня масштабованості і часу побудови таблиці маршрутизації в разі зміни топології великих телекомунікаційних мереж.

Для підвищення надійності телекомунікаційної мережі, було запропоновано використовувати додатковий мережевий протокол для підвищення надмірності та відмовостійкості мережі, шляхом відтворення віртуального роутера, який буде забезпечувати резервування і надавати додатковий логічний шлях, мережевий інтерфейс в разі відмови вузла, або лінії зв'язку в мережі.

Для виконання поставлених завдань, щодо підвищення надійності, були обрані наступні мережеві технології, які будуть використанні при моделюванні комп'ютерної цифрової мережі: HSRP, GLBP, ECMP, SNMP, VRRP.

У наступному розділі проводиться дослідження зі застосуванням віртуального середовища Cisco Packet Tracer для моделювання мережі, з вище перерахованими технологіями і приведенням порівняльного аналізу на основі результатів досліджень.

4 ДОСЛІДЖЕННЯ ВПЛИВУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

В рамках проведення досліджень по підвищенню надійності телекомунікаційної мережі пропонується метод дослідження впливу налаштування протоколів маршрутизації на надійність мережі.

Суть методу полягає в наступному: на основі обраних топологій мережі оцінити вплив різних конфігурацій мережі на час відновлення зв'язності мережі T_B .

З певних вимог побудови і функціонування мережі, були обрані протоколи динамічної маршрутизації.

Модель мережі побудована згідно трирівневої ієрархічної архітектури(рис.4.1):

Рівень ядра - вузли 1, 2, 3;

Рівень розподілу - вузли 4, 5, 6, 7, 8 та резервні вузли 11, 12;

Рівень доступу - вузли 9, 10;

Користувачі мережі - вузли U1, U2.

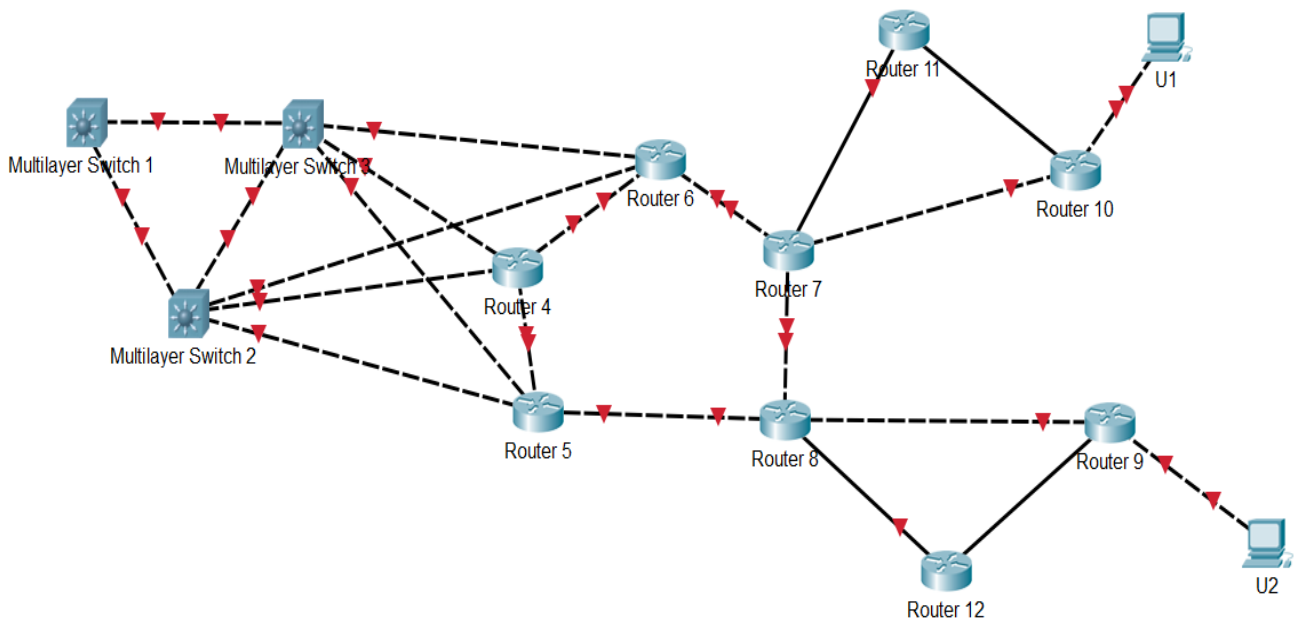


Рисунок 4.1 Архітектура мережі у ПО Cisco PT

Обладнання, яке використовується у моделюванні:

Для рівня ядра, використовуються комутатори 3-го рівня - з використанням програмного забезпечення Cisco IOS C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2;

Для рівня розподілу, використовуються маршрутизатори - з використанням програмного забезпечення Cisco IOS XE Version 03.16.05.S;

Для рівня доступу, використовуються маршрутизатори - з використанням програмного забезпечення Cisco IOS C1900 (C1900-UNIVERSALK9-M), Version 15.1;

Користувачі мережі - звичайні комп'ютери.

Для проведення досліджень, було прийнято, відключити один або два вузла розподілу і перевірити, з якою швидкістю, протокол маршрутизації замінить вузол з відмовою на резервний. У дослідженнях використовується мережа, змодельована в програмному середовищі Cisco Packet Tracer.

Аварія штучно викликається шляхом відключення одного вузла мережі. Для кожної з аварій вимірюється час відновлення зв'язності між вузлами абонентів підключених до вузлів 9 та 10.

Вимірювання часу відновлення зв'язності проводиться шляхом використання ICMP запитів з вузла одного абонента до іншого вузла. Кожна відповідь вузла абонента на один запит позначається виводом на термінал консолі вузла знаку «!», а кожне пропущене повідомлення «.». Тайм-аут для повідомлення виставлений 2 с, отже час відновлення $T_v = N * 2$ с, де N – кількість позначок «.» в поточному терміналі вузла абонента.

4.1 Дослідження впливу дистанційно-векторних протоколів маршрутизації

4.1.1 Модель з використанням протоколу RIP

В рамках досліджень, для першої моделі був обраний протокол RIP, як найпростіший протокол динамічної маршрутизації.

Протокол RIP заснований на дистанційно-векторному алгоритмі і в більшості реалізацій використовує найпростішу метрику - кількість проміжних маршрутизаторів до мережі призначення. У цьому протоколі всі мережі мають номери, а всі маршрутизатори - ідентифікатори. Протокол RIP широко використовує поняття "вектор відстаней". Вектор відстаней являє собою набір пар чисел, що є номерами мереж і відстанями до них в хопах.

До нових маршрутів маршрутизатори RIP пристосовується безболісно - вони передають нову інформацію в черговому повідомленні своїм сусідам і поступово ця інформація стає відома всім маршрутизаторам мережі.

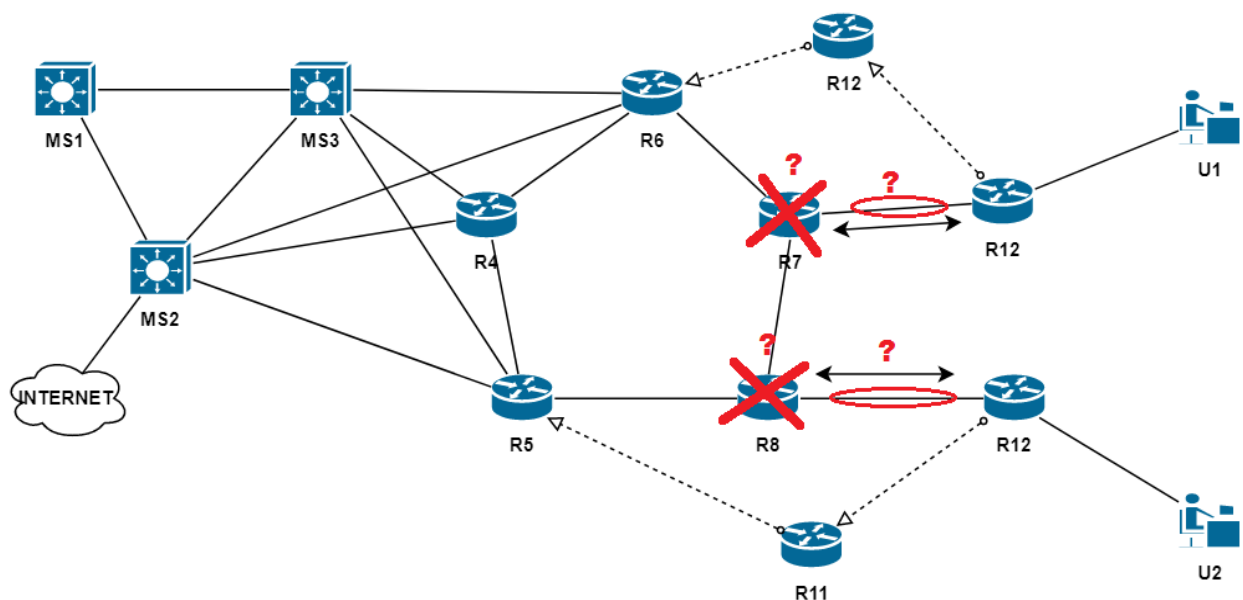


Рисунок 4.2 Модель мережі з використанням протоколу RIP

В даному випадку, при відключенні одного вузла, користувач мережі (U1 або U2) втрачає доступ до мережі. Протокол RIP при втраті будь-якого маршруту справляється досить проблематично. Це пов'язано з тим, що в форматі повідомлень протоколу RIP немає поля, яке б вказувало на те, що шлях до даної мережі більше не існує.

Для повідомлення про те, що даний маршрут недійсний, використовуються механізм закінчення часу життя маршруту.

Механізм заснований на тому, що обмін таблицями маршрутизації в протоколі RIP відбувається раз в 30 секунд, час тайм-ауту - в 6 разів більше, тобто 180 секунд, і маршрутизатор, який отримав повідомлення з підтвердженням запису маршруту, ставить таймер в початковий стан і якщо в плинні часу тайм-ауту (180 секунд) підтвердження не спадає ще раз, то маршрут стає недійсним.

RIP вимагає багато часу для відновлення зв'язку після збою в маршрутизаторі. В процесі встановлення режиму можливі цикли. Заміна пристрою, що відповідає за доступ до мережі, буде виконана через тривалий проміжок часу на резервний маршрутизатор. Другим головним недоліком цього протоколу, є його непрацездатність працювати у великих(глобальних) мережах.

При використанні протоколу RIP в трирівневій ієрархічній мережі, час відновлення вузла дорівнюватиме 190 с.

4.1.2 Модель з використанням протоколу IGRP

В рамках дослідження, для другої моделі був обраний протокол IGRP, як більш оптимальний протокол динамічної маршрутизації для підвищення надійності мережі.

Закритий дистанційно-векторний протокол IGRP компанії Cisco Systems був спроектований для усунення ряду недоліків протоколу RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з відмінними характеристиками смуги пропускання і величини затримки.

Протокол використовує комбіновану метрику, яка включає затримку, смугу пропускання, надійність і завантаженість маршруту.

Показники затримки і смуги пропускання конфігуруються для кожної лінії зв'язку попередньо, а показники надійності і завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі.

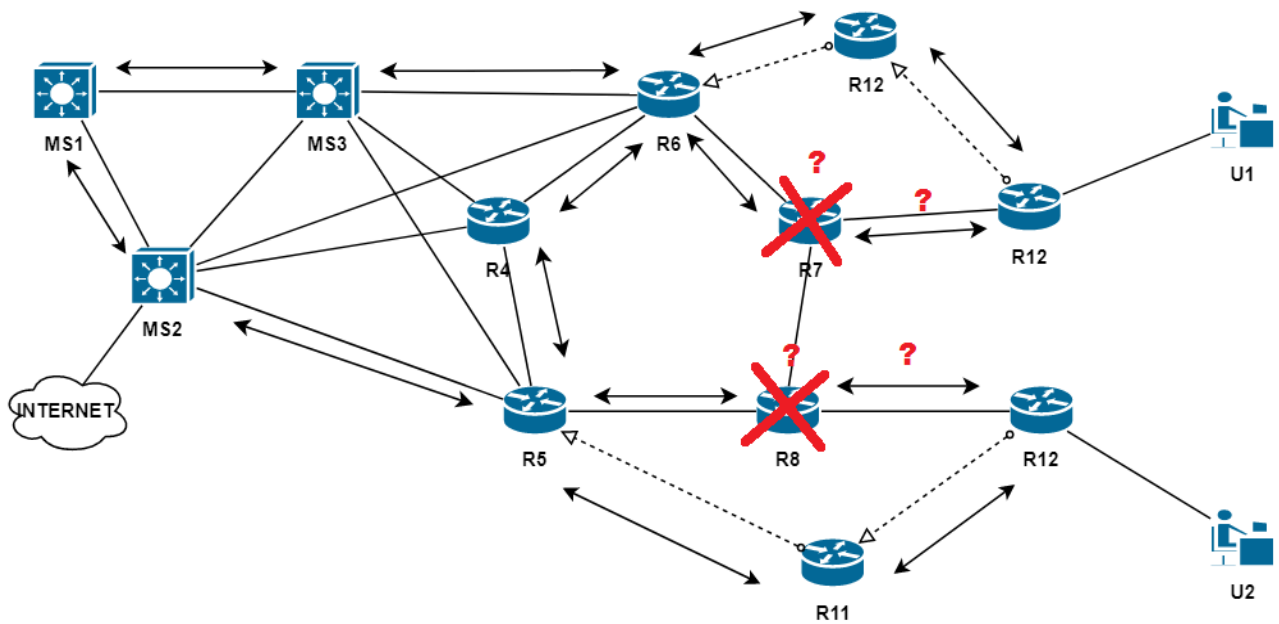


Рисунок 4.3 Модель мережі з використанням протоколу IGRP

В даному випадку, при відключенні одного вузла, користувач мережі (U1 або U2) втрачає доступ до мережі. Протокол IGRP при втраті будь-якого маршруту справляється спокійно. IGRP використовує широкомовні розсилки повідомлень з використанням періодичних таймерів (90с). Розсилаються повні копії своїх маршрутних таблиць.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини і можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні кошти аутентифікації при обміні маршрутною інформацією. Непрямим засобом захисту є можливість прийому повідомлень про оновлення маршрутів тільки від тих маршрутизаторів, які даний визначає як «сусідні», а також можливість внесення змін в конфігурацію маршрутизатора тільки на підставі пароля, який зберігається в зашифрованому вигляді.

При використанні протоколу IGRP в трирівневій ієрархічній мережі, час відновлення вузла дорівнюватиме 100 с.

4.2 Дослідження впливу протоколів маршрутизації за станом каналів

В рамках дослідження, для третьої моделі був обраний протокол OSPF, як один з найкращих протоколів динамічної маршрутизації на основі алгоритмів стану каналів.

Найбільш універсальним і гнучким у налаштуванні протоколом динамічної маршрутизації в корпоративних мережах на сьогоднішній день є відкритий протокол вибору першого найкоротшого шляху (Open Shortest Path First Protocol - OSPF).

Маршрутизатор під управлінням OSPF формує таблицю топології з використанням результатів обчислень, заснованих на алгоритмі найкоротшого шляху (SPF) Дейкстри. Алгоритм пошуку найкоротшого шляху ґрунтується на даних про сукупну вартість доступу до точки призначення.

Алгоритм пошуку найкоротшого шляху створює дерево найкоротших шляхів SPF шляхом розміщення кожного маршрутизатора в корені дерева і розрахунку найкоротших шляхів до кожного з вузлів. Після цього дерево найкоротших шляхів SPF використовується для розрахунку оптимальних маршрутів. Протокол OSPF вносить оптимальні маршрути в базу даних пересилання, яка застосовується для створення таблиці маршрутизації.

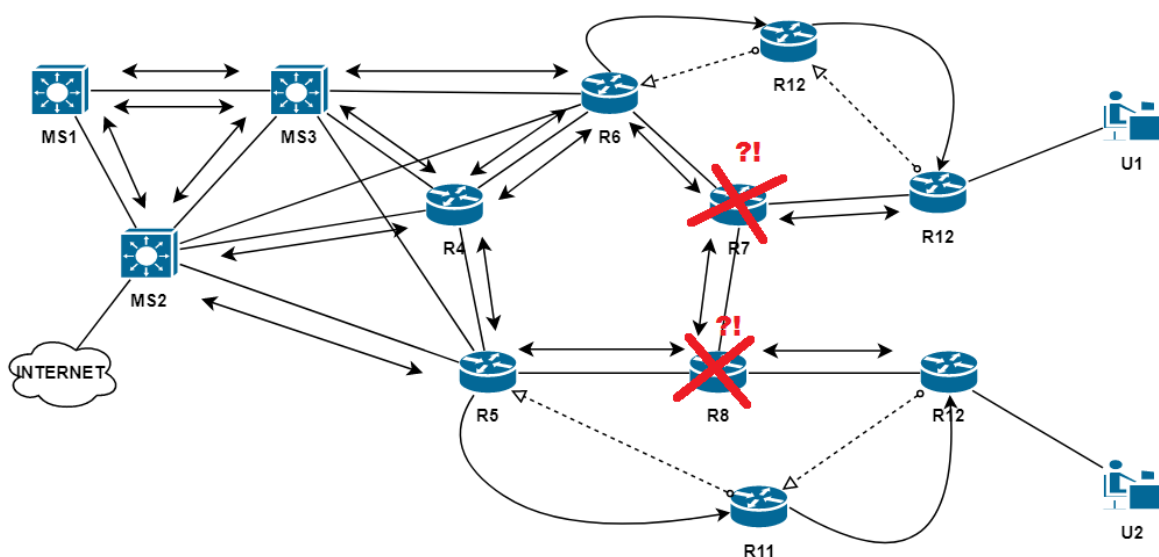


Рисунок 4.4 Модель мережі з використанням протоколу OSPF

В даному випадку, при відключенні одного вузла, користувач мережі (U1 або U2) втрачає доступ до мережі. Протокол OSPF реагує на це дуже швидко, завдяки розсилці пакетів Hello сусіднім маршрутизаторам.

Для протоколів стану зв'язків дуже важливим є те, щоб LSDB всіх маршрутизаторів були синхронізовані. При зміні будь-якого зв'язку маршрутизатори використовують механізм розсилки для повідомлення усіх маршрутизаторів зони. Для цього використовуються LSU, які поширюють нову LSA.

Процес збіжності в мережі під контролем протоколу OSPF, складається з наступних основних операцій:

- 1) виявлення відмови елемента мережі;
- 2) генерування нового LSA-повідомлення для оповіщення про нещодавно трапився зміні;
- 3) лавинна розсилка LSA-повідомлень в мережі;
- 4) виконання алгоритму пошуку найкоротших шляхів SPF на кожному маршрутизаторі, який отримує LSA-повідомлення;
- 5) оновлення таблиць маршрутизації LSDB на кожному маршрутизаторі за підсумками перерахунку SPF.

При використанні протоколу OSPF в трирівневій ієрархічній мережі, час відновлення вузла дорівнюватиме 50 с.

Протокол спочатку був орієнтований на роботу в великих мережах (до 65536 маршрутизаторів) зі складною топологією. Він заснований на алгоритмі стану каналів зв'язку і має високу стійкість до змін топології мережі і швидку збіжність з сусідніми вузлами. Платою за ці переваги є складність конфігурації і необхідність ретельного попереднього планування мережі для її оптимальної роботи.

4.3 Порівняльний аналіз протоколів маршрутизації на основі досліджень з використанням ПК Cisco Packet Tracer

Виходячи з аналізу та досліджень протоколів маршрутизації, можна сказати, що дистанційно-векторний протокол RIP поступається за цим параметром вдосконаленому протоколу IGRP. Ще більшою швидкістю збіжності має комбінований протокол EIGRP, який наближається до найбільш швидкісним протоколам OSPF і IS-IS, заснованим на алгоритмі обліку стану каналів зв'язку. Протокол BGP не відноситься до числа швидкісних, як через дистанційно векторного алгоритму, так і з огляду на його особливостей, пов'язаних з роботою в якості зовнішнього протоколу (різна маршрутна політика маршрутизаторів, використання надійного транспортного протоколу TCP і т.д.).

Дослідження показують, що найбільш досконалими внутрішніми протоколами динамічної маршрутизації є OSPF і IGRP. Протокол IS-IS по суті є більш ранній і менш функціональної версією протоколу OSPF, тому в даний час рідко використовується в корпоративних мережах. Переваги цих протоколів в повній мірі проявляються в складних великих мережах з сотнями і тисячами маршрутизаторів. Саме тут необхідна висока швидкість збіжності оптимальних маршрутів, гнучкість при виборі шляхів (з урахуванням різних характеристик, що складають маршрути каналів), підтримка вимог QoS для різних видів трафіку, економія смуги пропускання каналів (за рахунок зниження службового трафіку), зниження розмірів таблиць маршрутизації і швидкості пошуку в них інформації.

Ці вимоги виправдовують використання продуктивних апаратних маршрутизаторів з великими обсягами пам'яті і протоколів, що вимагають складної настройки. Однак такі великі мережі сьогодні є гетерогенними з точки зору виробників мережевого устаткування, тому лідируючі позиції тут займає відкритий протокол OSPF (EIGRP реалізується тільки на обладнанні Cisco Systems, і максимальну кількість маршрутизаторів не більше 255).

Протокол OSPF має кращу характеристику для роботи у великій мережі. Його принцип дії та адаптація, допомагає швидко знайти відмову у мережі. Якщо

мережа буде розширюватись, для протоколу OSPF це не є проблемою. OSPF використовує в таких випадках, поділ мережі на зони, що дозволяє зручно керувати розподіленими частинами великих мереж. Виходячи з досліджень, час відновлення вузла при використанні протоколу OSPF, дорівнюватиме 50 с.

4.4 Дослідження впливу на надійність телекомунікаційної мережі та порівняльний аналіз додаткових мережевих технологій

Для дослідження щодо підвищення надійності телекомунікаційної мережі з використанням додаткових мережевих технологій, був використаний протокол маршрутизації RIP, щоб протокол маршрутизації, не чинив великий вплив на час відновлення вузла.

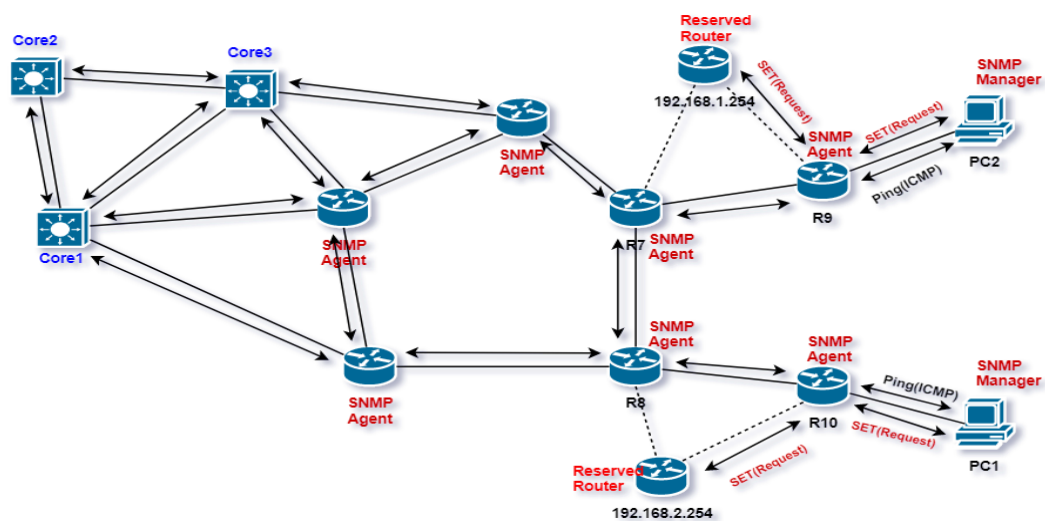


Рисунок 4.5 Модель мережі з використанням технології SNMP

1)SNMP

SNMP (Simple Network Management Protocol) - протокол, який використовується для управління мережевими пристроями. За допомогою протоколу SNMP, програмне забезпечення для управління мережевими пристроями може отримувати доступ до інформації, яка зберігається на керованих пристроях.

Виходячи з даних використаних ICMP запитів, було побудовано графік. В цьому графіку фіксується час відновлення вузла та проходження пакетів по каналам мережі.

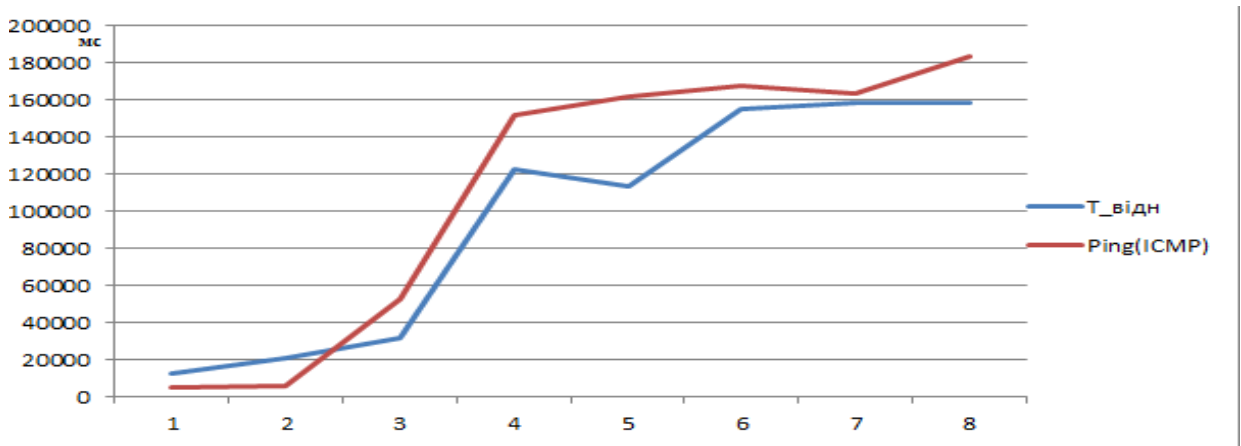


Рисунок. 4.6 Діаграма часу відновлення вузла та проходження ICMP-запитів по мережі

Виходячи з досліджень і отриманих результатів, які відображені в діаграмі часу відновлення вузла і проходження ICMP-запитів по мережі, бачимо що час відновлення вузла дорівнюватиме 120с, але, насамперед, час проходження пакета по мережі до вузла призначення, буде становити 160с.

2) ESMР

ESMP (Equal-cost multi-path routing) - це механізм, або навіть стратегія, коли в цілях доставки безлічі пакетів до єдиного одержувача ці пакети йдуть не через один best path, і не розподіляються через субоптимальні маршрути, а йдуть через кілька best path - зазвичай визначаються по метриці.

ESMP підвищує надійність мережі, шляхом балансування трафіку через різні шляхи. Але у випадку, якщо нам потрібно підвищити відмовостійкість мережі, це є недуже гарним варіантом. Для даної моделі, не використовуються резервні маршрутизатори.

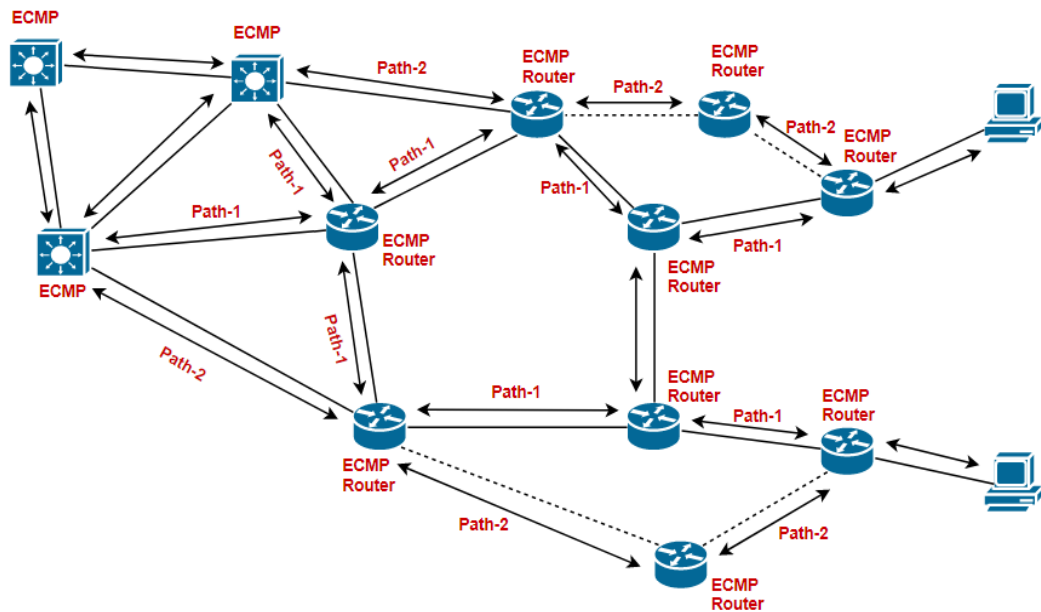


Рисунок 4.7 Модель мережі з використанням технології ECMP

Інтерфейси роутера, налаштовані на два шляхи і в разі виникнення відмов і переповнення трафіком маршрутів, він буде використовувати функцію балансування навантаження.

Тобто, якщо роутер до якого прокладений шлях-1 вийде з ладу, другий роутер від якого прокладений шлях-1, розподілить трафік на шлях-2 і буде передавати трафік до того моменту, поки роутер до якого прокладений шлях-1 не почне знову працювати.

Виходячи з даних використаних ICMP запитів, було побудовано графік. В цьому графіку фіксується час відновлення вузла та проходження трафіку по каналам мережі.

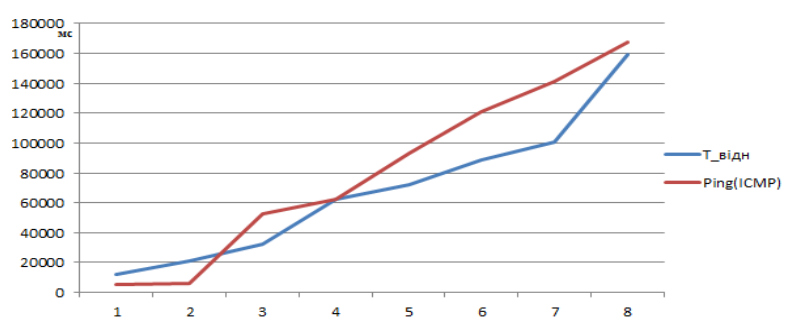


Рисунок 4.8 Діаграма часу відновлення вузла та проходження ICMP-запитів по мережі

Виходячи з досліджень і отриманих результатів, які відображені в діаграмі часу відновлення вузла і проходження ICMP-запитів по мережі, бачимо що час відновлення вузла дорівнюватиме 60с, але, насамперед, час проходження пакета по мережі до вузла призначення, буде становити 110с.

3)HSRP і VRRP

HSRP (Hot Standby Router Protocol) та VRRP (Virtual Router Redundancy Protocol) - це технології сімейства протоколів резервування першого переходу, іншими словами FHRP (FIRST HOP REDUNDANCY PROTOCOLS).

Дані технології були призначені для створення надмірності шлюзу. Загальною ідеєю для даних протоколів є об'єднання декількох маршрутизаторів в один віртуальний маршрутизатор із загальною IP адресою. Цей IP адрес буде призначатися на хостах як адрес шлюзу.

Схожість у даних технологій, дуже велика. Тому для даного дослідження, буде змодельована модель з використанням протоколу VRRP. Так як він, має більш високі переваги у зрівнянні з протоколом HSRP.

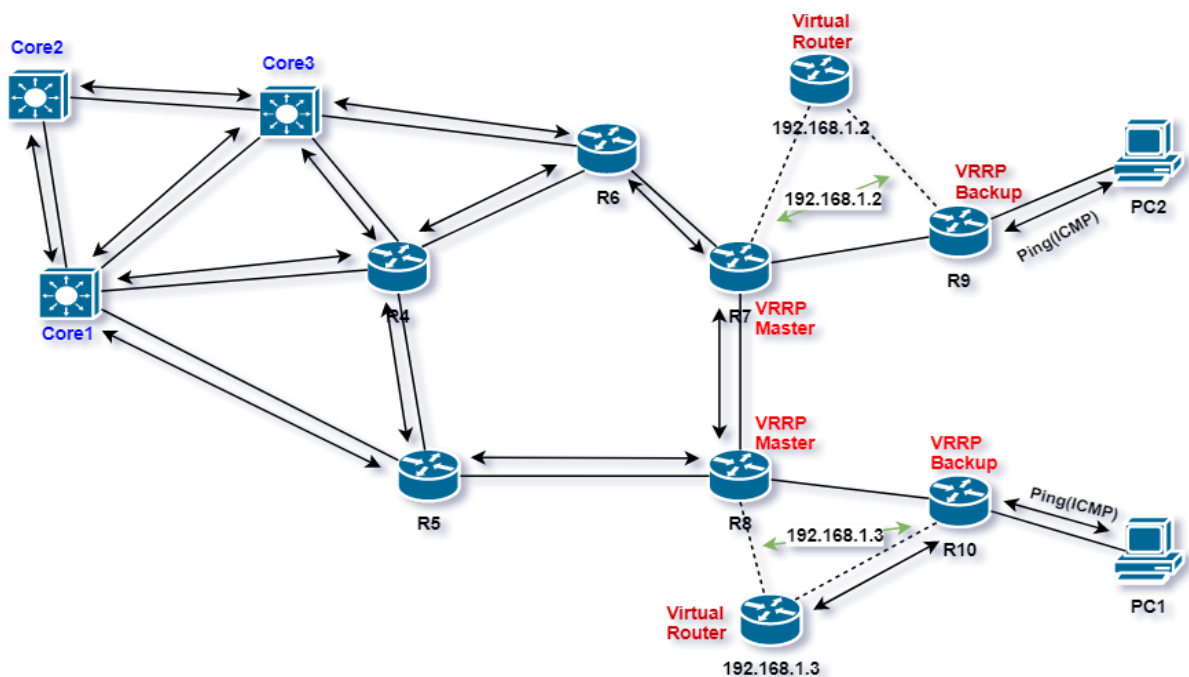


Рисунок 4.9 Модель мережі з використанням технології VRRP

У даній моделі використовується по два роутера на групу для створення віртуального шлюзу. Для цього об'єднуються групи маршрутизаторів в один віртуальний маршрутизатор і призначаються їм загальний IP-адресу, яка буде використовуватися як шлюз для комп'ютерів в мережі.

Один член групи вибирається активним маршрутизатором, в той час як інші залишаються неактивними до тих пір, поки не відбудеться збій з активним маршрутизатором.

У разі відмови маршрутного інтерфейсу роутера, трафік буде передаватися на віртуальний шлюз, через інший фізичний інтерфейс роутера.

При цьому ці резервні маршрутизатори мають ресурси, які майже не використовуються протягом всього часу експлуатації цієї системи.

Таким чином, технологія VRRP та HSRP підвищують надійність мережі, завдяки реалізації резервного шляху та створенню віртуального роутера.

Виходячи з даних використаних ICMP запитів, було побудовано графік. В цьому графіку продемонстровано фіксований час відновлення вузла та проходження трафіку по каналам мережі.

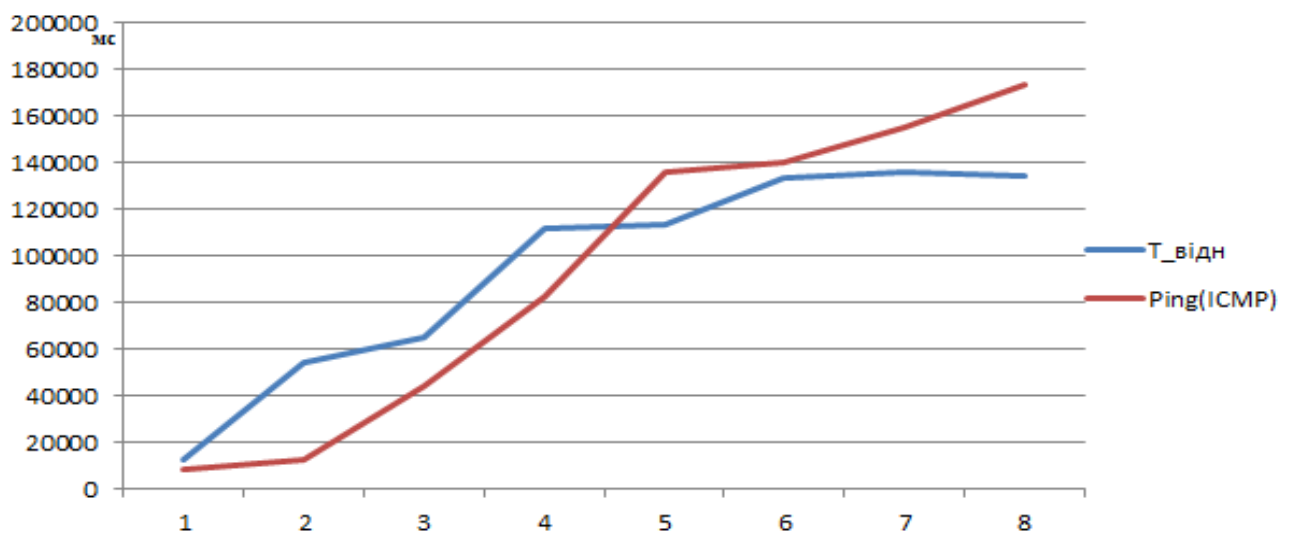


Рисунок. 4.1.1 Діаграма часу відновлення вузла та проходження ICMP-запитів по мережі

Виходячи з досліджень і отриманих результатів, які відображені в діаграмі часу відновлення вузла і проходження ICMP-запитів по мережі, бачимо що час відновлення вузла дорівнюватиме 55с, але, насамперед, час проходження пакета по мережі до вузла призначення, буде становити 100с.

4)GLBP

GLBP (Gateway Load Balancing Protocol) - пропрієтарний протокол Cisco, призначений для збільшення доступності маршрутизаторів виконують роль шлюзу і балансування навантаження між цими маршрутизаторами.

GLBP працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, такими як HSRP і VRRP. Ці протоколи дозволяють декільком маршрутизаторів брати участь в сконфігурованій віртуальній групі маршрутизаторів із загальним віртуальним IP-адресою.

GLBP забезпечує розподіл навантаження на декілька маршрутизаторів (шлюзів) використовуючи один віртуальний IP-адрес і кілька віртуальних MAC-адрес. Кожен хост налаштований з однаковим віртуальним IP-адресою і усі маршрутизатори у віртуальній групі беруть участь в передачі пакетів.

Члени групи GLBP вибирають один шлюз в якості активного віртуального шлюзу (AVG) для цієї групи. Інші члени групи забезпечують резервну копію AVG на випадок, якщо AVG стане недоступний. AVG призначає віртуальний MAC-адресу кожному члену групи GLBP. Кожен шлюз бере на себе відповідальність за пересилку пакетів, відправлених на віртуальний MAC-адресу, призначений йому AVG.

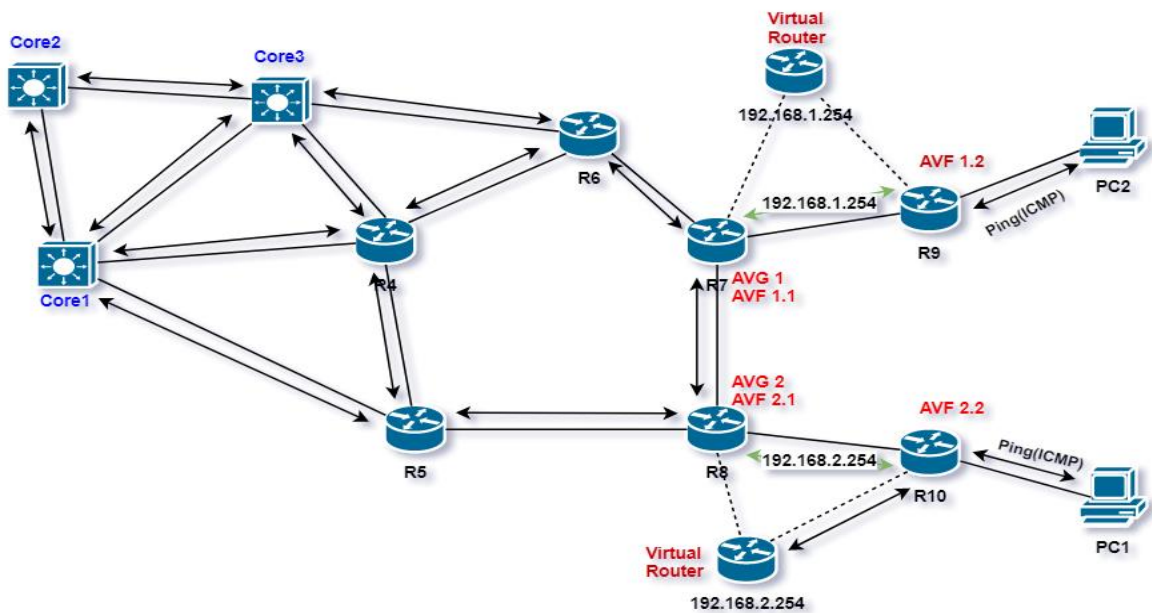


Рисунок 4.1.2 Модель мережі з використанням технології GLBP

GLBP управляє надмірністю віртуального шлюзу так само, як HSRP. Один шлюз вибирається як AVG, інший шлюз вибирається як резервний віртуальний шлюз, а решта шлюзи переводяться в стан прослуховування. У разі збою AVG резервний віртуальний шлюз бере на себе відповідальність за віртуальний IP-адреса. Потім з шлюзів в стані прослуховування вибирається новий резервний віртуальний шлюз.

Резервування віртуального сервера пересилання схоже на резервування віртуального шлюзу за допомогою AVF.

У разі збою AVF один з вторинних віртуальних серверів пересилки в стані прослуховування приймає на себе відповідальність за віртуальний MAC-адресу. Новий AVF також є основним віртуальним сервером пересилання для іншого номера сервера пересилання. GLBP переносить вузли зі старого номера сервера пересилання за допомогою двох таймерів, які запускаються, як тільки шлюз переходить в активний стан віртуального сервера пересилання. GLBP використовує привітальні повідомлення для передачі поточного стану таймерів.

Час перенаправлення - це інтервал, протягом якого AVG продовжує перенаправляти хости на старий MAC-адресу віртуального сервера пересилання. Після закінчення часу перенаправлення AVG припиняє перенаправлення хостів на

віртуальний сервер пересилання, хоча віртуальний сервер пересилання буде продовжувати пересилати пакети, відправлені на старий MAC-адресу віртуального сервера пересилання.

Вторинне час утримання - це інтервал, протягом якого діє віртуальний сервер пересилання. Коли час вторинного утримання закінчується, віртуальний сервер пересилання видаляється з усіх шлюзів в групі GLBP. Номер віртуального сервера пересилання з вичерпаним терміном дії може бути перепризначений AVG.

Виходячи з даних використаних ICMP запитів, було побудовано графік. В цьому графіку продемонстровано фіксований час відновлення вузла та проходження трафіку по каналах мережі.

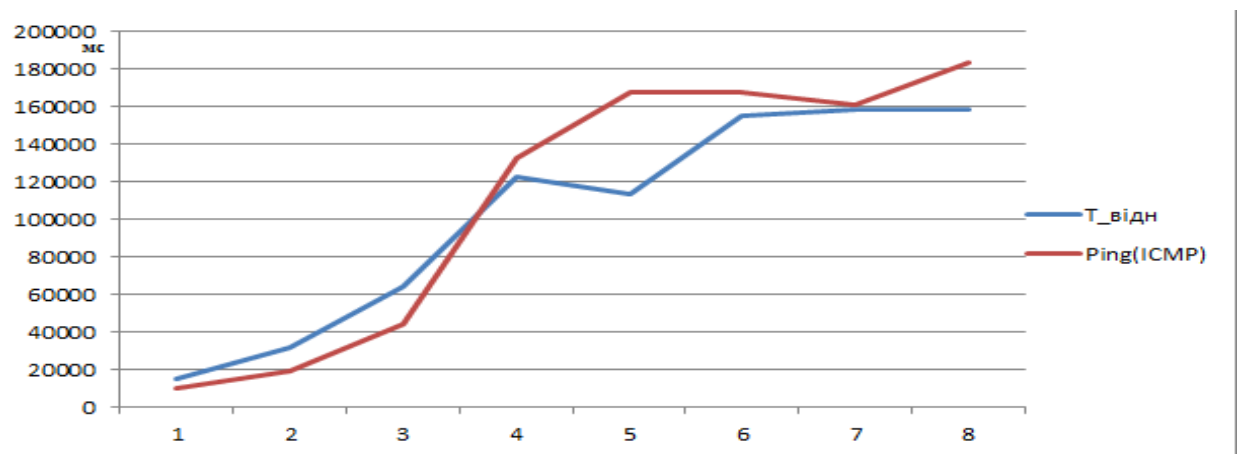


Рисунок 4.1.3 Діаграма часу відновлення вузла та проходження ICMP-запитів по мережі

Виходячи з досліджень і отриманих результатів, які відображені в діаграмі часу відновлення вузла і проходження ICMP-запитів по мережі, бачимо що час відновлення вузла дорівнюватиме 50с, але, насамперед, час проходження пакета по мережі до вузла призначення, буде становити 100с.

4.5 Дослідження впливу протоколу маршрутизації OSPF з використанням додаткового мережевого протоколу

В рамках заключного дослідження по завданню про підвищення надійності мережі, було запропоновано використовувати в зв'язці дві технології. Для маршрутизації трафіку і перестроювання таблиці маршрутизації в мережі, використовується протокол OSPF. Протокол OSPF, виходячи з досліджень, довів що він один з кращих протоколів динамічної маршрутизації, який досить швидко реагує на зміни в мережі і перебудовує топологію по всьому мережевому домену, шляхом використання широкомовної розсилки.

Для спільної роботи з протоколом OSPF та для підвищення надійності мережі використовується протокол GLBP. Дана технологія, дозволяє регулярно балансувати навантаження в мережі, в разі якщо якийсь канал зв'язку буде перевантажений. Також, дана технологія, істотно дозволяє підвищити відмовостійкість мережі. У разі обриву лінії або відмови вузла, дана технологія реалізує віртуальний роутер, шляхом об'єднання кількох мережевих інтерфейсів. Це створює можливість, мати в резерві ще один шлях, тобто, надає віртуальний логічний канал, по якому можливо передавати мережевий трафік.

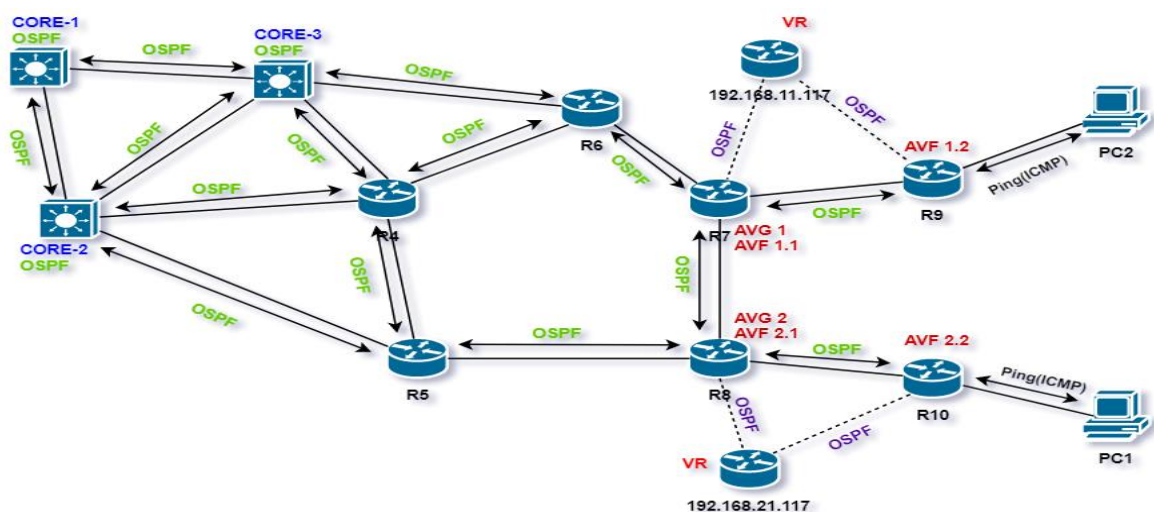
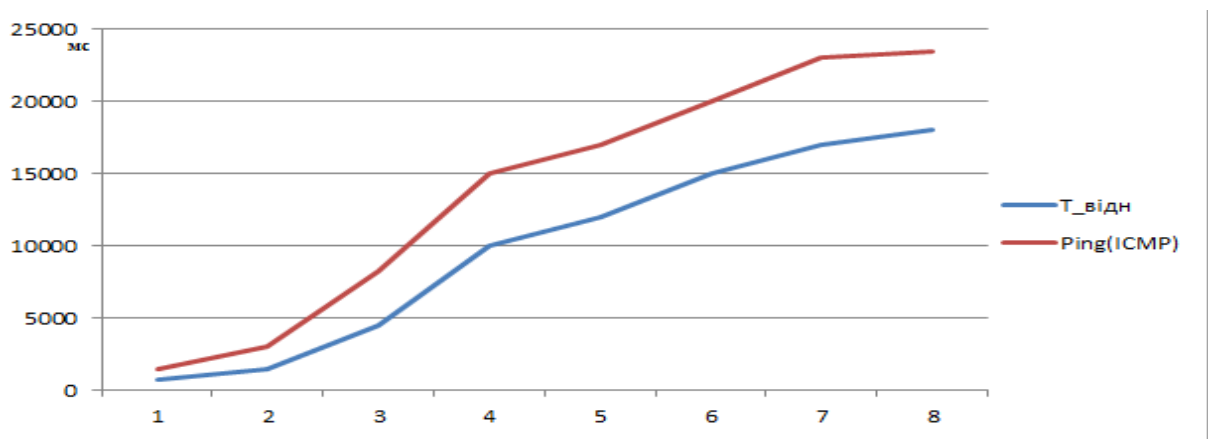


Рисунок 4.9 Модель з використанням протоколу OSPF та GLBP



Таблиця 4.1.4 Діаграма часу відновлення вузла та проходження ICMP-запитів по мережі

Виходячи з досліджень і отриманих результатів, які відображені в діаграмі часу відновлення вузла і проходження ICMP-запитів по мережі, бачимо що час відновлення вузла дорівнюватиме 10с, але, насамперед, час проходження пакета по мережі до вузла призначення, буде становити 15с.

4.6 Висновки до розділу 4

В рамках досліджень, щодо впливу протоколів маршрутизації на надійність телекомунікаційної мережі, була змодельована мережа в програмному середовищі Cisco Packet Tracer. При дослідженні, були використані протоколи динамічної маршрутизації, як за станом каналу, так і дистанційно векторні. Також, для підвищення надійності мережі, було запропоновано використовувати додаткову мережну технологію, яка буде впливати на відмовостійкість мережі, в разі ненавмисних збоїв або відмов мережевих вузлів.

Аварія створюється штучно, шляхом відключенням однієї лінії зв'язку. Після раптового виникнення аварії, протокол динамічної маршрутизації який використовується в мережі, створює широкомовну розсилку до всіх сусідніх маршрутизаторів про зміни топології в мережі. Після того, як кожен маршрутизатор отримує повідомлення про те, що маршрут в мережі був змінений, він починає процес реконфігурації таблиці маршрутизації. Також, в даному

дослідженні, була поставлена задача, підвищити надійність телекомунікаційної мережі. Даним показником при дослідженні, були обрані показники відмовостійкості мережі та її надлишковість у разі відмови лінії зв'язку.

Для цього дослідження, був використаний протокол GLBP, спільно з протоколом динамічної маршрутизації станом каналу OSPF. Ці дві технології, добре доповнюють один одного, при інтегруванні їх і взаємної роботі в мережі. Протокол OSPF, має найменший час збіжності в порівнянні з іншими протоколами маршрутизації і час зміни таблиці маршрутизації всередині одного мережевого домену або декількох. Для підвищення надійності мережі, протокол GLBP створює ряд переваг.

Протокол GLBP дозволяє декільком маршрутизаторів брати участь в віртуальній групі маршрутизаторів з загальною віртуальною IP-адресою. Один член групи вибирається активним маршрутизатором, в той час як інші залишаються неактивними до тих пір, поки не відбудеться збій з активним маршрутизатором. При цьому ці резервні маршрутизатори мають ресурси, які не використовуються протягом всього часу експлуатації цієї системи. GLBP забезпечує розподіл навантаження на декілька маршрутизаторів (шлюзів) використовуючи один віртуальний IP-адреса і кілька віртуальних MAC-адрес. Кожен хост налаштований з однаковою віртуальною IP-адресою і всі маршрутизатори у віртуальній групі беруть участь в передачі пакетів.

Виходячи з вищесказаного, при дослідженні впливу протоколів маршрутизації на надійність телекомунікаційної мережі і поставленого завдання щодо підвищення надійності при використанні додаткових мережевих технологій, були отримані наступні результати:

1. При використанні додаткових технологій, сумісно з протоколом маршрутизації RIP, були отримані наступні результати:

- При використанні SNMP та протоколу RIP, час відновлення вузла дорівнюватиме 120с, а час проходження пакета по мережі до вузла призначення, буде становити 160с.

- При використанні VRRP та протоколу RIP, час відновлення вузла дорівнюватиме 55с, а час проходження пакета по мережі до вузла призначення, буде становити 100с.

- При використанні ECMP та протоколу RIP, час відновлення вузла дорівнюватиме 60мс, а час проходження пакета по мережі до вузла призначення, буде становити 110мс.

- При використанні GLBP та протоколу RIP, час відновлення вузла дорівнюватиме 50мс, а час проходження пакета по мережі до вузла призначення, буде становити 100мс.

2. При використанні протоколу OSPF за станом каналу і протоколу GLBP, були отримані наступні результати:

- При використанні GLBP та протоколу OSPF, час відновлення вузла дорівнюватиме 10с, а час проходження пакета по мережі до вузла призначення, буде становити 15с.

ВИСНОВКИ

В рамках виконання магістерської дисертації на тему "Дослідження впливу протоколів маршрутизації на надійність телекомунікаційної мережі", було розглянуто принципи побудови сучасних телекомунікаційних мереж, їх класифікація та типи фізичних топологій, які використовуються у наш час в цифровому просторі.

Було обґрунтовано, що надійність телекомунікаційної мережі повинна забезпечувати клієнтам можливість обмінюватися інформацією і отримувати сервіси в умовах технічних відмов, експлуатаційних помилок, а також з урахуванням можливих загроз і ризиків, пов'язаних з атаками типу відмова в обслуговуванні.

Було розглянуто, що таке маршрутизатор, які функції маршрутизатор виконує в мережі, на основі яких даних він будує свою таблицю маршрутизації та для чого вона використовується. Також, були розглянуті вимоги мережі до протоколу маршрутизації для повноцінного розуміння при виборі протоколу маршрутизації та введенням його в експлуатацію з якісною працездатністю в мережі.

В рамках дослідження впливу протоколів маршрутизації на надійність телекомунікаційної мережі, пропонується метод нарощування надмірності мережі за допомогою резервних шляхів, шляхом штучного введення їх в мережу та віртуальних логічних каналів, які будуть утворені при використанні додаткових мережевих технологій.

Для підвищення надійності телекомунікаційної мережі, було запропоновано використовувати додатковий мережевий протокол для підвищення надмірності та відмовостійкості мережі, шляхом відтворення віртуального роутера, який буде забезпечувати резервування і надавати додатковий логічний шлях, мережевий інтерфейс в разі відмови вузла, або лінії зв'язку в мережі.

Для оцінки надійності мережі, буде використовуватися час відновлення вузла, шляхом використання ICMP запитів та фіксацією часу їх проходження по мережі, відправлених з одного вузла на інший.

Для кінцевого дослідження, був використаний протокол GLBP, спільно з протоколом динамічної маршрутизації за станом каналу OSPF. При використанні GLBP та протоколу OSPF, час відновлення вузла дорівнюватиме 10с, а час проходження пакета по мережі до вузла призначення, буде становити 15с. Тобто, виходячи з результатів досліджень, можна сказати, що протокол OSPF і протокол GLBP при сумісній роботі в мережі, можуть забезпечити і підвищити надійність телекомунікаційної мережі. Єдиним недоліком є те, що протокол GLBP вважається пропрієтарним протоколом і працює виключно на обладнанні фірми CISCO.

В рамках магістерської дисертації з дослідження впливу протоколів маршрутизації на надійність мережі, була поставлена задача про забезпечення і підвищення надійності мережі. Виходячи з досліджень при використанні різних технологій, був проведений порівняльний аналіз і були наведені результати в діаграмі проходження ICMP запитів. Виходячи з діаграми проходження ICMP запитів, завдання про забезпечення і підвищення надійності мережі, було успішно виконано.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — 4 изд. — СПб. : Питер, 2010. — ISBN: 9785498073897.
2. Cisco Systems. Руководство по междоменной многоадресатной маршрутизации. — 1 изд. — СПб. : Вильямс, 2004. — 320 с. — ISBN: 5845906059.
3. Алексеев Е.Б., Данилов А.Н., Матвеев В.А., Грош А.О. Анализ протоколов маршрутизации в сетях NGN.
4. Jacek Rak, Mario Pickavet, Kishor S. Trivedi, Javier Alonso Lopez, Arie M. C. A. Koster, James P. G. Sterbenz, Egemen K. Çetinkaya, Teresa Gomes, Matthias Gunkel, Krzysztof Walkowiak & Dimitri Staessens. Telecommunication Systems. [Электронный ресурс] - Режим доступа до ресурсу:
<https://link.springer.com/article/10.1007/s11235-015-9987-7>
5. Килячков К.П. МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ.
6. В.А. БАЧИНСКИЙ, В.Ш. ГИОРГИЗОВА-ГАЙ. ВЫБОР ПРОТОКОЛА ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ В КОРПОРАТИВНОЙ IP-СЕТИ.
7. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ
8. М.А. Павленко, М.Ю. Гусак, Д.О. Калиновський. АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ
9. Данилюк И.П. Повышение надежности инфокоммуникационных сетей.
10. R. Hinden. RFC 3768 - Virtual Router Redundancy Protocol [Электронный ресурс] - Режим доступа до ресурсу:
<https://tools.ietf.org/html/rfc3768>
11. Cisco Systems. Gateway Load Balancing Protocol [Электронный ресурс] - Режим доступа до ресурсу:
https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
12. J.Case., M. Fedor., M. Schoffstall., J. Davin. RFC 1157 - Simple Network Management Protocol [Электронный ресурс] - Режим доступа до ресурсу:

<https://tools.ietf.org/html/rfc1157>

13. С. Хоппс. NextHop Technologies. RFC 2992 - Analysis of an Equal-Cost Multi-Path Algorithm [Электронный ресурс] - Режим доступа до ресурсу:

<https://tools.ietf.org/html/rfc2992>

14. Т. Ли., В. Коле., Р. Мортон., Д. Ли. RFC 2281 - Cisco Hot Standby Router Protocol [Электронный ресурс] - Режим доступа до ресурсу:

<https://tools.ietf.org/html/rfc2281>